TEST PILOT SCHOOL

AIRBORNE SYSTEMS COURSE

TEXTBOOK

ELECTRONIC WARFARE SYSTEMS

TEST AND EVALUATION

GLOSSARY MATERIAL

18 March 1981

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER –	2. GOVT ACCESSION NO. AD-A130 536	3. RECIPIENT'S CATALOG NUMBER –
4. TITLE (and Subtitle) Electronic Warfare Systems Test and Evaluation		5. TYPE OF REPORT & PERIOD COVERED –
		6. PERFORMING ORG. REPORT NUMBER –
7. AUTHOR(s) George W. Masters		8. CONTRACT OR GRANT NUMBER(s) –
9. PERFORMING ORGANIZATION NAME AND ADDRESS U. S. Naval Test Pilot School Naval Air Test Center Patuxent River, Maryland 20670		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS –
11. CONTROLLING OFFICE NAME AND ADDRESS Academics Branch U. S. Naval Test Pilot School		12. REPORT DATE 18 March 1981 13. NUMBER OF PAGES 101
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) –		15. SECURITY CLASS. (of this report) UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE –

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

–

18. SUPPLEMENTARY NOTES

–

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Electronic Warfare, Electronic Countermeasures, Jamming, Avionics, Airborne Systems, Weapon Systems, Test and Evaluation, Flight Testing

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

Textbook for use in teaching test and evaluation of electronic warfare systems including theory of operation, operating characteristics, and test methodology. Topics include electronic reconnaissance, electronic countermeasures, electronic counter-countermeasures, electronic warfare system parameters, and test methods.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

ELECTRONIC WARFARE SYSTEMS

TEST AND EVALUATION

TABLE OF CONTENTS

ELECTRONIC WARFARE SYSTEM TEST AND EVALUATION

1.0 Introduction

Electronic warfare could be defined to include all use of electronic devices in warfare. The commonly employed definition, however, is more restrictive. The term "electronic warfare" is generally assumed to include only those devices designed to interfere with, or prevent such interference with, the operation of military systems that employ electromagnetic communications links. (In accordance with the material presented in the text on communications, the definition of a "communications link" is here assumed to include all systems that convey information from one point to another. This definition includes voice and data links, electromagnetic remote sensors such as radar and infrared detectors, and radio navigation systems.) At the present time, the most extensive employment of electronic warfare is concerned with radar systems. For that reason, this text approaches the subject of electronic warfare primarily from the radar viewpoint. It should be noted, however, that all of the principles and almost all of the techniques discussed in connection with radar are directly applicable to the other "communications" systems. Similarly, although the subject of this text is electronic warfare as it applies to airborne systems, the principles and techniques discussed herein are generally applicable to land and sea-based systems as well. The principal EW targets are the systems listed below.

Target Detection Systems
Target Tracking Systems
Surface-to-Air Weapon Delivery Systems
Air-to-Air Weapon Delivery Systems
Missile Homing and Fuse Systems
Ground Controlled Intercept Systems
Communication Systems
Navigation Systems
Electronic Warfare Systems

The sensors employed in these systems utilize both radio-frequency and optical-frequency electromagnetic waves and perform both passive and active detection. Target detection systems include early warning radars, search and acquisition radars, infrared detectors, and low-light-level television detectors. Target tracking systems include tracking radars, missile guidance radars, infrared trackers, low-light-level television trackers, and laser trackers and designators. Surface-to-air weapon delivery systems include surface-to-air missile (SAM) launch and guidance systems and anti-aircraft artillery (AAA) gun directors. Air-to-Air weapon delivery systems include various types of radar-guided missile systems, radar gunsight systems, passive home-on-radar and home-on-jam systems, and electro-optical missile guidance and homing systems. Ground controlled intercept systems include both the target tracking system and the interceptor command and control communications link. Communication systems include voice and data links. The navigation systems susceptible to electronic countermeasures are those which utilize electromagnetic radiation for sensing or communication. Such systems include radio navigation systems, command link guidance systems, Doppler radar navigation systems, and systems which utilize radar, infrared, or visible radiation for terrain sensing. Electronic warfare systems include intercept receivers, radar and missile-launch warning systems, noise (denial) jammers, and deception jammers.

As indicated above, the subject of electronic warfare is concerned with the "communications" systems previously defined. For that reason, almost all of the theoretic background material necessary to understand electronic warfare is presented in the texts on communication systems, radar systems, electro-optical systems, and radio navigation systems. Only the theory peculiar to electronic warfare techniques is contained in this text. The reader is referred to the texts mentioned above for the background theory not presented herein.

Most of the information describing actual, currently-employed, electronic warfare equipment is classified. For that reason, such material is not included in this text. For that information, the reader is referred to the separate, classified volume describing current weapons systems.

Electronic warfare (EW) encompasses three distinct activities: electronic reconnaissance (ER), electronic countermeasures (ECM), and electronic counter-countermeasures (ECCM). Electronic reconnaissance is that branch of electronic warfare involved in gathering, by electronic means, information concerning the intentions and operations of the adversary and the capabilities and characteristics of his "communications" equipment. Electronic countermeasures is that branch of electronic warfare involved in degrading the usefulness of the adversary's "communications" equipment. Electronic counter-countermeasures is that branch of electronic warfare involved in preventing the electronic countermeasures of the adversary from degrading the usefulness of "communications" equipment employed by friendly forces.

The field of electronic warfare is characterized by a rapid evolution of techniques. Within a short time after one side introduces a new technique, the other side develops a counter-technique. The pace of the evolutionary process is a measure of the importance placed upon electronic warfare by the modern military. Early ECM primarily employed the relatively unsophisticated methods of noise jamming. Then, as the practitioners of electronic warfare became more proficient in ECM, the emphasis shifted to deception jamming. Then, as the practitioners became more proficient in ECCM, the emphasis shifted again to noise jamming. (Noise jamming is more ECCM resistant.) The application of spread-spectrum techniques is making effective ECM ever more difficult. At the same time, important

improvements are being made in real-time signal analysis and signal generation. It seems likely, however, that the simplicity, universality, and ECCM resistance of noise jamming will ensure a continuing role for that ECM technique despite its lack of sophistication.

For purposes of electronic countermeasures, the threats commonly encountered by an airborne vehicle can be divided into three categories: early warning, area defense, and point defense. Early warning systems are primarily long-range search radars. Area defense systems are primarily long-range surface-to-air missiles (SAM's) and ground controlled intercept (GCI) systems. Point defense systems are primarily short-range surface-to-air missiles and anti-aircraft artillery (AAA). Although the roles of the three types of threats overlap to some extent, and the various systems are interactive as a result of exchange of information, the electronic countermeasures appropriate to each type differ considerably. The principal reason for the differences is the immediacy of the threat in time and space. Other differences are due to dissimilarities in the characteristics of the threat systems, such as those of search as opposed to track radars.

2.0 Electronic Warfare Theory

2.1 Electronic Reconnaissance

2.1.1 Levels of ER -- The gathering of information in support of electronic warfare activities takes place at three levels: the strategic level, the tactical level, and the combat level.

Strategic ER is generally called electronic intelligence (ELINT) and is a long-term process involving large amounts of data and extensive analysis. ELINT data are usually acquired by long-range signal-monitoring (intercept) receivers from positions removed from the combat zone and are typically used in the design of EW equipment and to perform strategic planning.

Tactical ER, generally called electronic support measures (ESM), is concerned with the gathering of information for use in current (daily) operations. The intercept equipment is generally located (at least temporarily) in the combat zone and the analysis of the data is more-or-less limited to determining the locations and types of equipment currently deployed by the adversary. As the name implies, tactical ER data is used to perform tactical planning and to adjust EW equipment to meet current threats.

Electronic reconnaissance at the combat level, (also generally called ESM), is concerned with identification of immediate threats and targets. The information is collected and analyzed for immediate use. Because of the urgency, data analysis and presentation are usually automated and, therefore, minimal. An example of combat ESM equipment is the ALR-45/50 radar warning receiver (RWR) system installed in tactical aircraft.

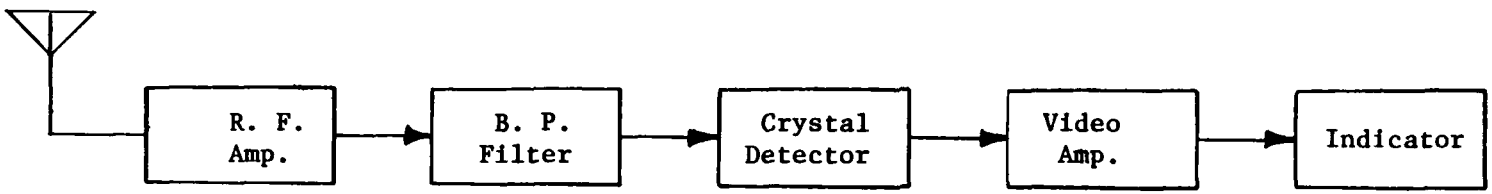
2.1.2 Characteristics of EW Target Systems -- In order to apply effective countermeasures against a specific threat system, it is necessary to determine the significant characteristics of that system. Significant characteristics include those listed below.

Location (Direction)
Effective Radiated Power
Polarization
Antenna Pattern
Scanning Pattern
Frequency Spectrum
Modulation
Pulse Repetition Frequency
Pulse Width
Angle Track Method
Frequency Stability
Frequency Agility
PRF Agility
Operational Characteristics
Missile Guidance Type
Missile Fuse Type
Electronic Counter-countermeasures
Type of System (Search Radar, SAM, AAA, etc.)
Specific Equipment
Mode of Operation (Search, Track, Weapon Launch, etc.)

Determination of the above characteristics is required in order to identify the source of the radiation (the threat) and to devise suitable countermeasures.

2.1.3 Electronic Reconnaissance Intercept Receivers -- Electronic reconnaissance equipment consists of intercept receivers, signal analyzers, and indicators. Intercept receivers are of two basic types: direct detection receivers and superheterodyne receivers. The direct detection receiver employs no intermediate frequency, the radio frequency signal being directly detected to audio or video frequency. The block diagram for a direct detection receiver with R.F. tuning and preamplification is shown in Figure 2.1.3.1(a). The advantages of a direct detection receiver are simplicity and wide bandwidth. The bandwidth is determined

(a) Tuned Direct Detection Receiver



2.1a

(b) Superheterodyne Receiver

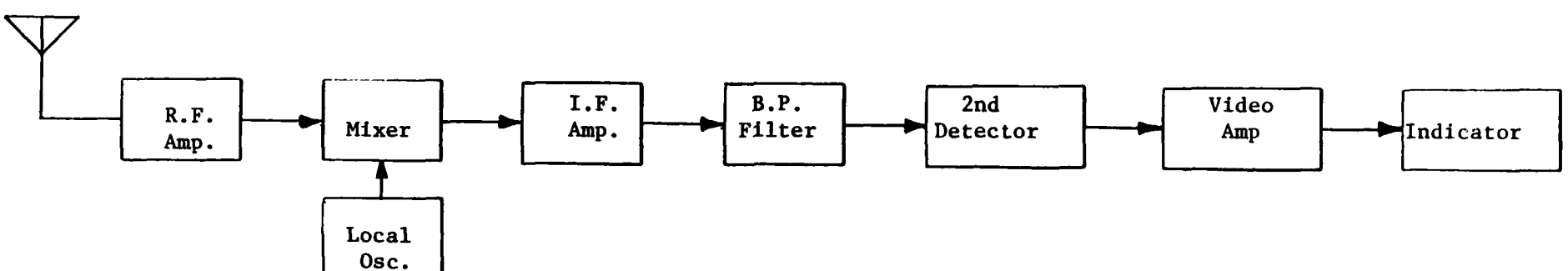


Figure 2.1.3.1 -- Electronic Reconnaissance Receivers

by the tuner (bandpass filter). Some wideband receivers employ no tuner, the bandwidth then being determined only by other components such as the antenna. The disadvantages of direct detection receivers are relatively low sensitivity and, generally, poor frequency selectivity. The alternative to the direct detection receiver is the superheterodyne receiver, shown in Figure 2.1.3.1(b). The superheterodyne receiver offers better sensitivity and better frequency resolution when needed.

2.1.4 Electronic Reconnaissance Signal Analysis -- The frequency of the intercepted signal can be determined by tuning the bandpass filter shown in Figure 2.1.3.1(a); by sweeping the frequency of the local oscillator shown in Figure 2.1.3.1(b); or by employing multiple tuned channels as shown in Figure 2.1.4.1. When rapid frequency determination is required, the multiple-channel approach must be employed or the frequency scanning (or tuning) must be done electronically rather than mechanically.

The direction-of-arrival of the intercepted signal can be determined by using a narrow-beam, scanning antenna or by using multiple antennas. Multiple, narrow-beam antennas driving individual indicators, as shown in Figure 2.1.4.2, can be used to obtain an angular resolution dependent upon the number of antennas. Amplitude-comparison or phase-comparison (interferometer) arrangements, such as the four-antenna system shown in Figure 2.1.4.3, can be used to obtain precise direction-of-arrival information employing relatively few wide-beam antennas. (See Sections 2.3.5 and 2.17.6 of the radar text for discussion of amplitude and phase comparison techniques).

The type(s) of modulation present in an intercepted signal of unknown characteristics can be determined by the sequential selection process indicated in

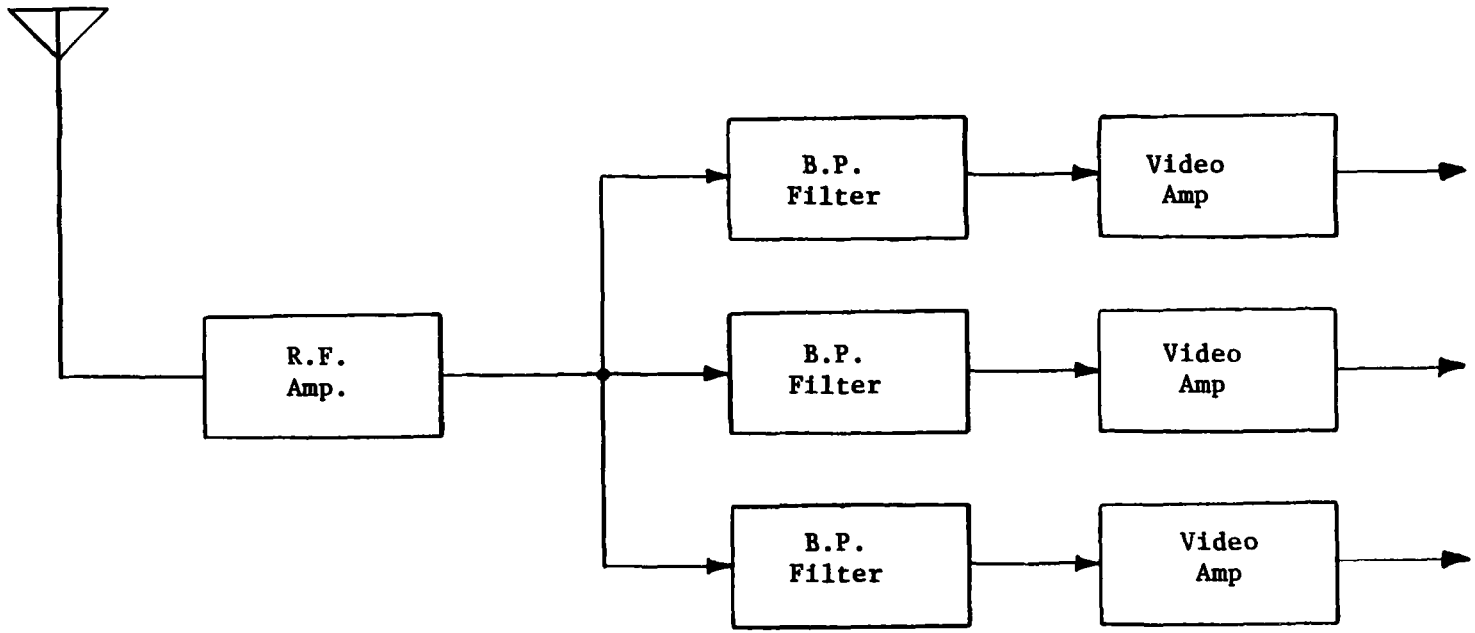


Figure 2.1.4.1 -- Multiple-Channel Direct Detection Receiver

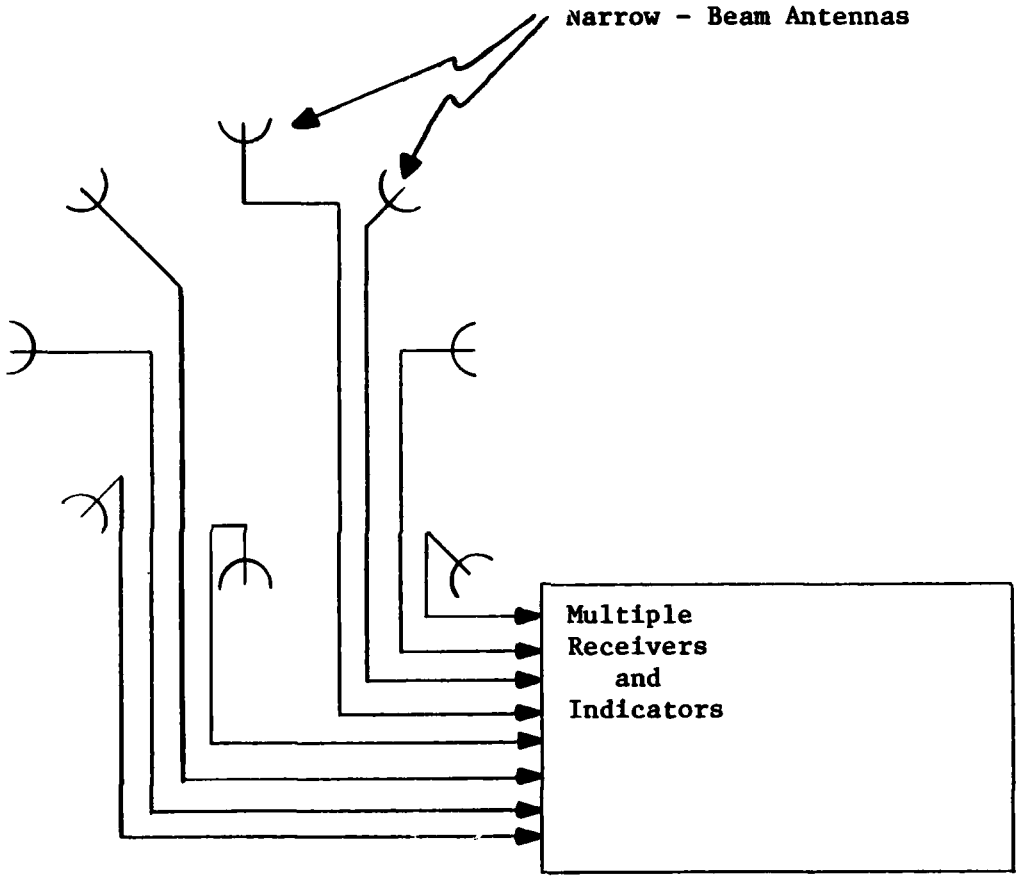


Figure 2.1.4.2 -- Multiple-Channel Direction-of-Arrival Determination

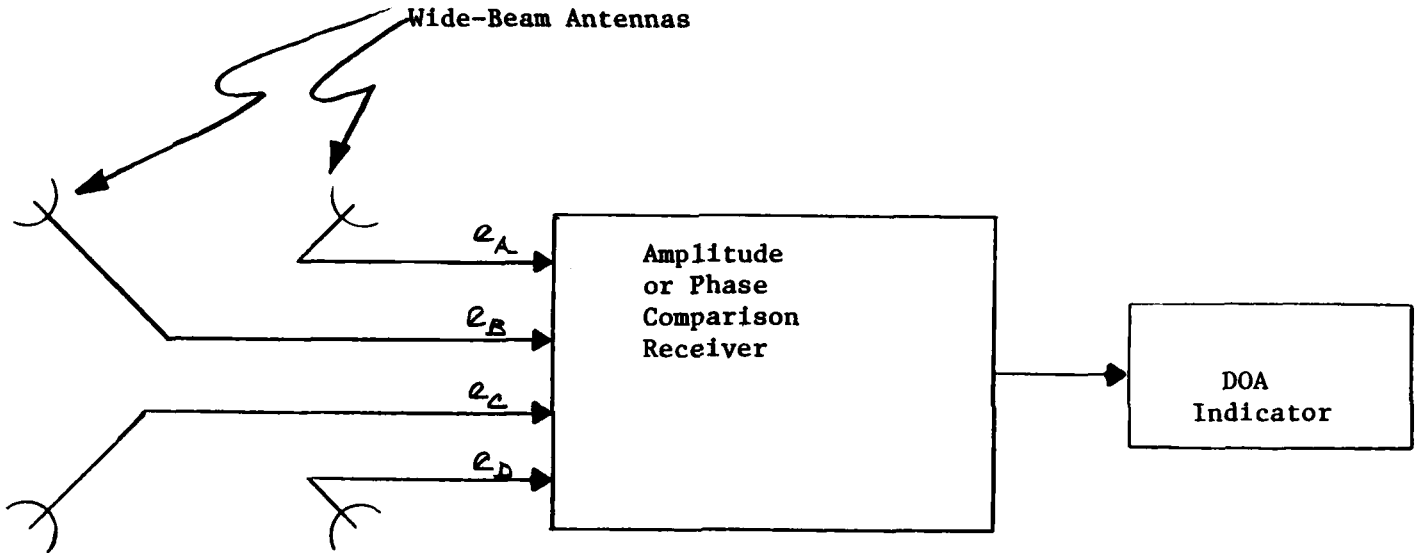


Figure 2.1.4.3 -- Amplitude Comparison or Phase Comparison Direction-of-Arrival Determination

Figure 2.1.4.4. When the parameters of a signal of known modulation type are to be determined, a general screening process such as that shown is not required.

The detailed parameters of an intercepted signal (pulse width, pulse repetition interval, scan rate, etc.) can be determined in both the time domain (signal time-sequence analysis) and in the frequency domain (spectral analysis). In the time domain, intervalometers and counters are employed to measure pulse widths and time intervals directly. In the frequency domain, these parameters are inferred from spectral characteristics. (For example, the width of the spectral lines of a pulsed signal is a measure of the pulse width and the spacing between the spectral lines is a measure of the pulse repetition interval). Signals containing multiple (interleaved) pulse trains can be analyzed by identifying individual pulse trains and deleting them, one at a time, from the signal. For threat identification systems, parameter identification must be followed by correlation of the parameter values with those of known threats. The advent of digital signal processing greatly improved the parameter identification and correlation capabilities of airborne, real time signal analyzers. The block diagram for a digital radar homing and warning (RHAW) receiver is shown in Figure 2.1.4.5.

A primary consideration in the field of electronic reconnaissance is the probability of intercepting a given threat signal. That probability is a function of the characteristics of both the threat and the intercept receiver. The major factors influencing probability of intercept are listed below.

Threat Signal-to-Background Noise Ratio
Threat Signal Duty Cycle
Threat Signal Spectrum
Threat Antenna Beamwidth (If Directional)
Threat Antenna Scan Pattern and Rate

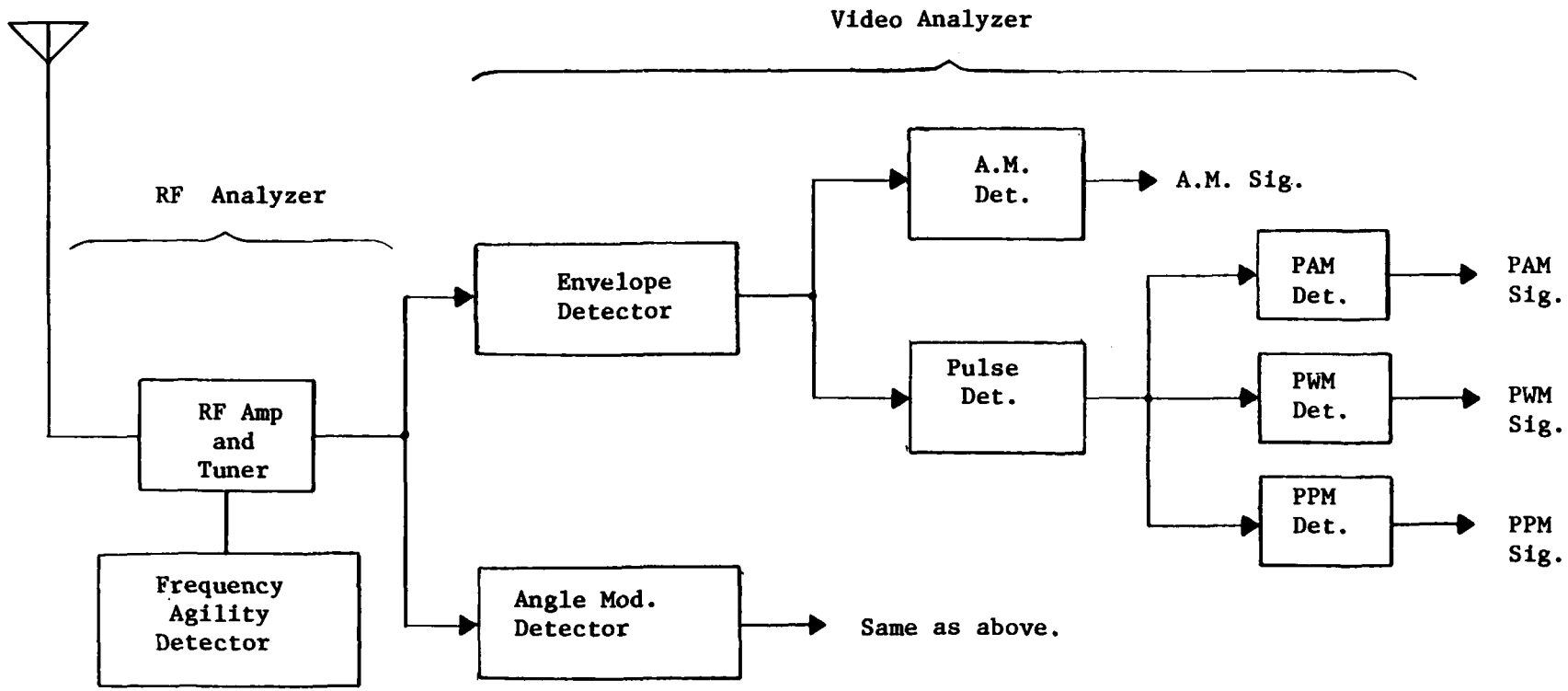


Figure 2.1.4.4 -- Electronic Reconnaissance Modulation Detector

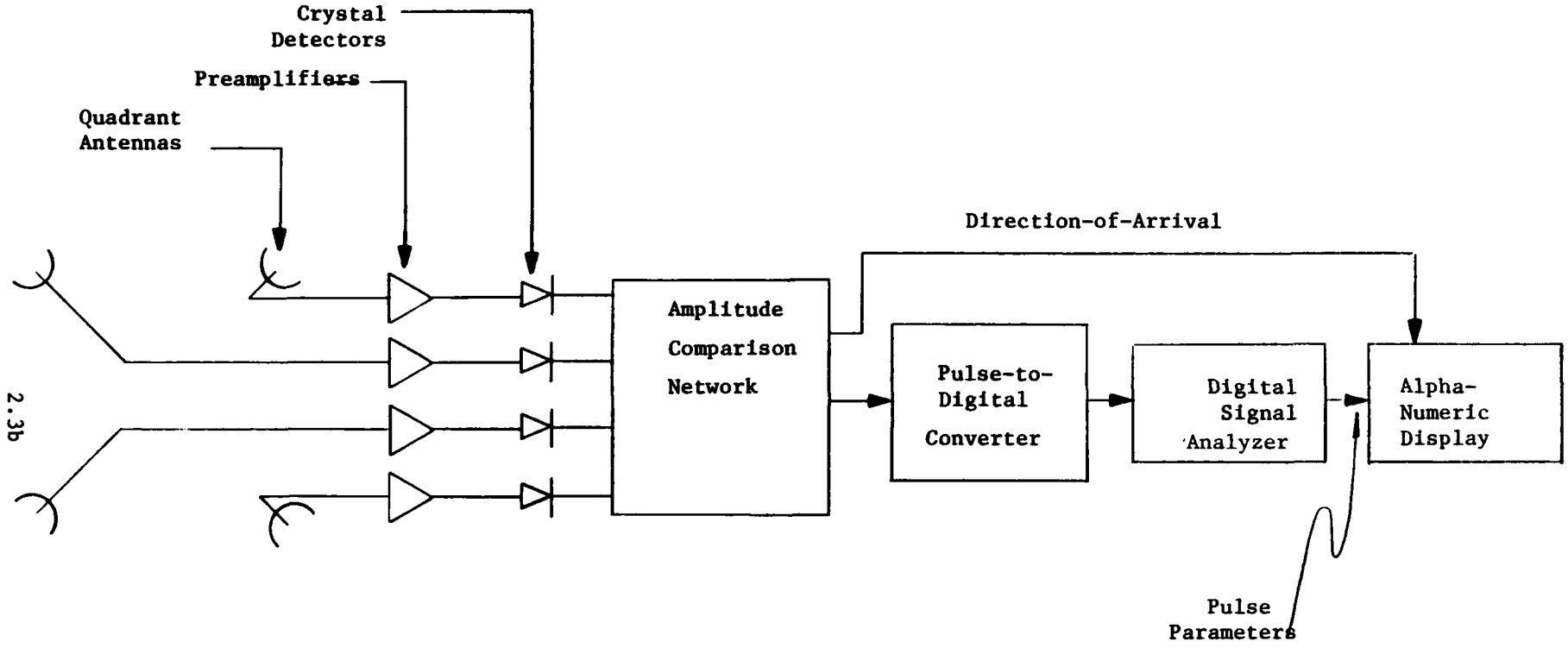


Figure 2.1.4.5 -- Radar Homing and Warning Receiver

Threat Parameter Agility
Receiver Threshold Sensitivity
Receiver Bandwidth (If Tuned)
Receiver Frequency Scan Rate
Receiver Response Time
Receiver Antenna Beamwidth (If Directional)
Receiver Antenna Scan Pattern and Rate
Receiver Signal Processing Gain

It should be noted that, generally, multiple coincidence (frequency, antenna position, etc.) is required for signal detection.

A major problem associated with electronic reconnaissance systems is that of "look-through". That is, the problem of preventing friendly sensors, jammers, and communication links from "jamming" the intercept receiver. In general, continuing observation of the threat signals is necessary for effective electronic countermeasures. Since friendly jammers ordinarily operate at the frequencies monitored by the receivers, avoiding interference by frequency separation usually is not possible. The two principal techniques employed to provide for intercept receiver look-through are antenna isolation and time multiplexing (signal blanking). Since the interference in question is that between friendly (cooperative) units, it often is possible to employ directive antennas with sufficient isolation to avoid the problem. Blanking of the interfering signal at the input of the intercept receiver can be effected either by programmed time multiplexing or by detecting the transmitting periods of the interfering equipment and gating off the input to the receiver during those periods. Because of the difficulty in turning the jamming transmitter off, it is sometimes merely de-tuned during the "off" period, thus eliminating its interference with the receiver. An alternative method of eliminating jamming transmitter-to-receiver interference is to utilize a portion of the transmitter output to generate a signal identical to the interference signal and opposite in phase, and using it to cancel the interfering signal in the receiver.

2.2 Electronic Countermeasures

2.2.1 ECM Techniques -- The principal electronic countermeasures techniques are listed below.

Non-Radiating ECM Techniques

Threat Avoidance
Threat Saturation
Threat Destruction
Threat Intimidation
Vehicle Emission Reduction
Vehicle Cross-Section Reduction
Use of Chaff and Rope

Radiating ECM Techniques

Noise Jamming
Deception Jamming
Use of Expendable Jammers
Use of Active Decoys

As indicated, ECM techniques fall into two broad categories: radiating and non-radiating. These categories, however, are not mutually exclusive. For example, threat system saturation can be achieved by the use of passive (non-radiating) decoys or by the use of an active (radiating) deception jammer (described below).

2.2.2 Non-Radiating ECM -- The ECM techniques that do not involve the radiation of electromagnetic signals are discussed in the following paragraphs.

Threat Avoidance -- Threat avoidance, when feasible, is an attractive option because it involves no ECM radiation, expends no stores (e.g. chaff), and provides the adversary with a minimum of electronic intelligence. Although it employs no specialized ECM equipment, it does utilize, and is heavily dependent upon, electronic reconnaissance equipment.

Threat Saturation -- Threat saturation is the technique of providing the adversary with so many apparent targets (real or false) that he is unable to cope with the real targets effectively. The intent is not to obscure the real targets but, rather, to dilute the defenses of the adversary. The "apparent" targets can be real targets, decoys, (possibly with cross-section enhancing reflectors), or false targets due to deception jamming.

Threat Destruction and Intimidation -- Threat destruction and intimidation are related. That is, it is the possibility of destruction that intimidates the threat into ceasing operation. As a result of intimidation, the effectiveness of such weapons as anti-radiation missiles is much greater than that implied by the (severely limited) number of missiles actually available.

Emission Reduction -- Emission reduction is possible in both the radio frequency and optical regions of the spectrum. Reduction of radio frequency emissions can be effected by limiting or eliminating the use of radiating equipment (radars, Doppler navigators, radar altimeters, communication systems, etc.). Effective reduction of emissions also can be achieved by the use of spread-spectrum techniques as discussed in the section on electronic counter-countermeasures. Emissions in the optical region can be reduced by non-reflective coatings and by designing structures to shield light sources from optical sensors. Reduction of infrared radiation can be achieved by non-radiative coatings, cooling of heated structures, structural shielding of heated structures, and shielding exhaust gases by structures or a cooler sheath of gas.

Cross-Section Reduction -- Two major non-actively radiating techniques are employed to modify the effective cross section of aircraft: structural design and the use of anti-reflective coatings. Planar and angular (non-curved) surfaces and structures of dimension equal to one-half wavelength or more tend to reflect electromagnetic radiation in a directive manner. Curved surfaces tend to diffuse the reflected radiation. For that reason, it is possible to effect a significant reduction in radar cross section by avoiding planar and angular configurations in the structural design of an aircraft. It is also possible to design an aircraft with planar structures so oriented as to reflect radiation away from the radiating source, again decreasing the effective cross section. Anti-reflective coatings are of two types. One type absorbs (dissipates) the radiant energy as it propagates through the coating. The other type utilizes destructive interference between the reflections from two or more layers in the coating to decrease the radiation reflected back toward the source. Both types of antireflective coating add substantially to the size and weight of the aircraft.

Chaff and Rope -- Chaff consists of thin strips of a conductive material cut to a length equal to one-half of the wavelength of the radiation to be reflected. Each strip of chaff is thus a combination receiving and transmitting (reflecting) half-wave dipole antenna. (Radiation absorbing chaff also is possible.) Like all such antennas, it is both frequency and orientation dependent. The frequency dependence is accommodated by cutting the chaff to various lengths as needed. The orientation dependence is overcome by dispensing large quantities of chaff, the overall effect of the chaff "cloud" being omnidirectional. For low frequencies, long-lengths of chaff, called "rope" are employed. The advantages of chaff are its simplicity, wide applicability, and relative resistance to ECCM. Its disadvantages are its expendability and its restricted spatial coverage.

Protection is afforded only in the immediate vicinity of the cloud. If extensive coverage is required, large amounts of chaff must be dispensed creating a chaff "blanket" or "corridor". The time duration of protection is limited by the prevailing winds and by the fact that the chaff falls under the influence of gravity. The low weight-to-aerodynamic drag ratio of chaff prevents it from falling rapidly, but it also causes the chaff to assume the velocity of the airmass almost immediately upon being dispensed. The resulting difference in velocity between the chaff and the aircraft allows a Doppler radar to distinguish between the target aircraft and the chaff.

2.2.3 Radiating ECM -- Radiating ECM systems employ two basic principles: obscuration of the information signal and generation of false information signals. When the target system is a radar, the first method conceals the true target returns. The second method makes no attempt to conceal the true targets but provides false information to disrupt the system being jammed. The first method is the brute-force approach, essentially denying to the adversary the use of the target system. The second method is the more subtle approach, merely preventing effective use of the system. In this text, the first method is called noise jamming; the second method is called deception jamming.

Noise Jamming -- The name "noise" jamming derives from the fact that noise jammers generally employ a noise-like modulation on the jamming signal. No attempt is made to duplicate all characteristics of the true target returns since the intent is merely to "out-shout" them. (It should be noted that a noise jamming signal can "obscure" a true target return even when it is not superimposed directly upon the target return. By affecting the automatic gain control in the target

system, the noise jamming signal can reduce the gain of the system to the point where the true target return is not discernible.) The main disadvantage of noise jamming is the difficulty of generating sufficient power within the bandwidth of the victim receiver to obscure the true target returns. Even when the frequency of the jammed system is known and the jammer is tuned to that frequency, noise jamming is a relatively inefficient use of power. Because the jamming signal must actually obscure the target returns, a much larger power is required than for deception jamming. When the precise frequency of the jammed system is unknown or when several frequencies must be jammed simultaneously, an even larger power is required. The main advantage of noise jamming is the minimal amount of intelligence required for effective jamming. Only the location and transmission frequency of the target system are required, and even those sometimes need be known only approximately. The inherent insensitivity of noise jamming to detailed information on the characteristics of the target system also implies an insensitivity to ECCM, since changes in most of the system characteristics are of no significance.

There are three types of noise jammers in common use: the spot jammer, the broadband (barrage) jammer, and the swept-spot (swept frequency) jammer. The spot jammer generates a narrow-bandwidth, noise-like cw signal tuned to the frequency of the system to be jammed. (The bandwidth of a spot jammer is ideally matched to that of the target system). Spot jamming is the most power-efficient method of noise jamming a single target system of known frequency. Its principal disadvantage with respect to the other types of noise jamming is the requirement for relatively precise knowledge of the frequency of the system to be jammed.

The broadband jammer overcomes the requirement for precise knowledge of the frequency of the target system by generating a relatively broad-bandwidth signal. (The bandwidth is typically greater than ten percent of the center frequency). Thus, only a general knowledge of the target system frequency is required. The power spectral density of a broad-band noise jammer is, of course, considerably less than that of a spot jammer, the bandwidth of which may be only one or two percent of the center frequency.

The third type of noise jammer is the swept-spot jammer. The swept-spot jammer combines the broad-bandwidth characteristic of the broad-band jammer with the power spectral density of the spot jammer by sweeping the center frequency of the spot through a frequency range of, perhaps, two-to-one. Thus, the swept-spot jammer requires only a very general knowledge of the target system frequency. An important advantage of the swept-spot jammer is its ability to jam several systems simultaneously. The principal disadvantage of the swept-spot jammer is the fact that it jams any one system only intermittently. If the dwell time in the frequency bandwidth of the target system or the sweep repetition rate is not large enough, the target system will recover between sweeps.

There are a number of methods used to generate pseudo-noise signals. The most direct method is to band-limit the thermal noise generated in a reverse-biased diode (or other noisy component) and amplify the resulting signal directly. The band-limited noise can be converted to any desired portion of the spectrum or swept in center frequency by heterodyning. The most common method of generating a noise-like signal is wideband frequency modulation of a carrier with noise processed to produce a jamming signal with a spectrum flat over the frequency band of interest. The effect of noise jamming on a radar PPI display is depicted in Figure 2.2.3.1.

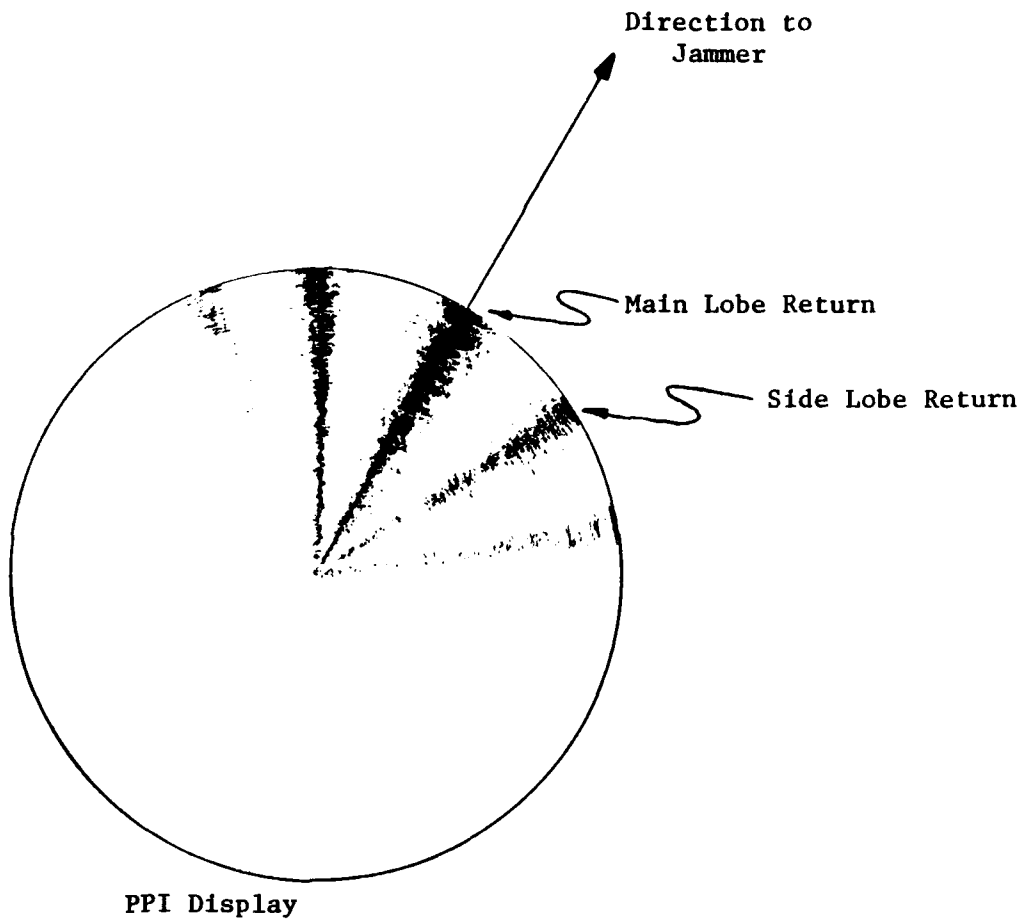


Figure 2.2.3.1 -- Appearance of Noise Jamming on Radar PPI Display

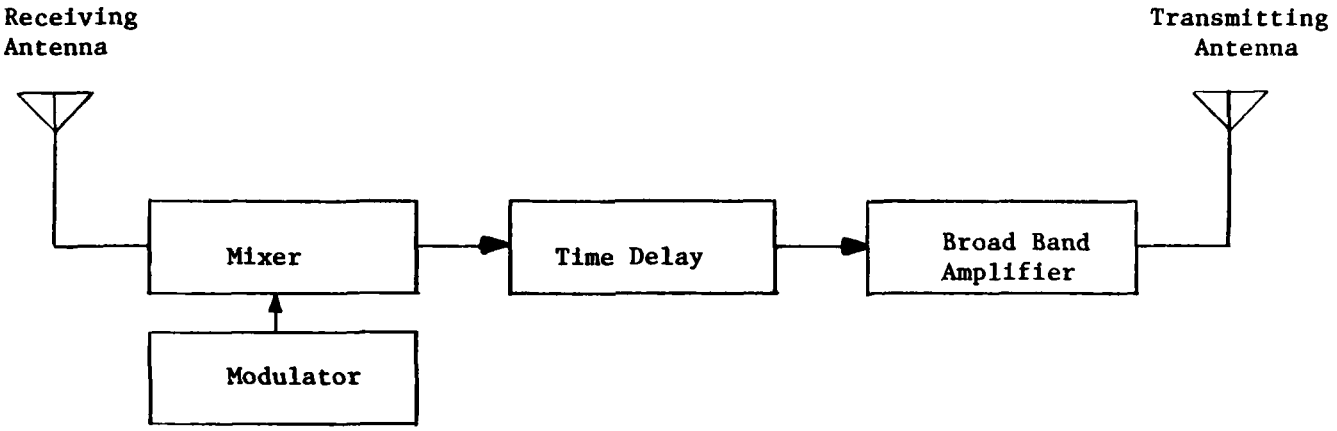
Deception Jamming -- As previously stated, the intent of deception jamming is not to obscure the true target returns but to generate false information in such a way as to disrupt the operation of the jammed system. In order for such false information to be accepted by a radar system, it must possess the characteristics of true target returns. For example, it must possess the proper carrier frequency, pulse width, pulse repetition frequency, scan characteristics, and other modulation. The generation of such a deception signal requires a detailed knowledge of the parameters of the target system. That information must be acquired by the methods of electronic reconnaissance discussed in Section 2.1 of this text. The information must be current and, if the parameters are varying due to ECCM, they must be updated in real time. (When pseudo-random parameter variations are employed for ECCM, it may be impossible to update the parameter values in real time.) The requirement for detailed, continuously updated information on the jammed system is the most important disadvantage in deception jamming. The most important advantage of deception jamming, over noise jamming, is the much lower power required. For a pulsed target system signal, the output of a deception jammer is pulsed, with a duty cycle similar to that of the jammed signal. For the same target system, the output of a noise jammer must be continuous, with a power equal to the peak power of the jammed signal. Another important advantage over noise jamming is the fact that deception jamming can be covert. With noise jamming, the adversary is usually aware that he is being jammed and can apply counter-countermeasures.

There are two basic methods of deception jamming: the false-target generator and the track breaker. The false-target generator produces false target returns indistinguishable from the true returns, thereby saturating the jammed system. The track breaker disrupts range, velocity, and angle tracking systems.

False-Target Generators -- False-target generators are of two kinds: repeaters and transponders. The repeater receives the target system signal, perhaps delays and/or modifies it, and retransmits it. The essential characteristics of the received signal are preserved in the transmitted signal by virtue of the fact that they are the same signal, (perhaps with certain modifications). Thus, a repeater is able to match the target system signal without detailed a-priori information as to its characteristics and without detailed real-time signal analysis. The block diagram of a typical "straight-through" repeater is shown in Figure 2.2.3.2(a). The signal from the target system is continuously received, modified and/or delayed as required, amplified, and re-transmitted. Destabilizing feedback is prevented by providing sufficient isolation between the transmitting antenna and the receiving antenna. The block diagram of a gated repeater is shown in Figure 2.2.3.2(b). In the gated repeater, the receiving and transmitting functions are alternately enabled (gated) to prevent feedback. Since the receiving and transmitting periods do not overlap, the time delay shown in the diagram is required as memory. When jamming of more than one target system (frequency) is required, a swept-frequency repeater can be employed. The block diagram of a swept-frequency repeater is shown in Figure 2.2.3.3. The effect of the swept local oscillator, mixers, and narrow-band I.F. amplifier is to pass only one received signal (frequency) at a time. Thus, any one target system is jammed only intermittently by this method.

The amplitudes of the false target returns produced by the repeaters shown in Figures 2.2.3.2a and 2.2.3.2b will vary in accordance with target system signal strength. Thus, as the target system scans, a symmetric false target pattern

(a) Straight - Through Repeater



(b) Gated Repeater

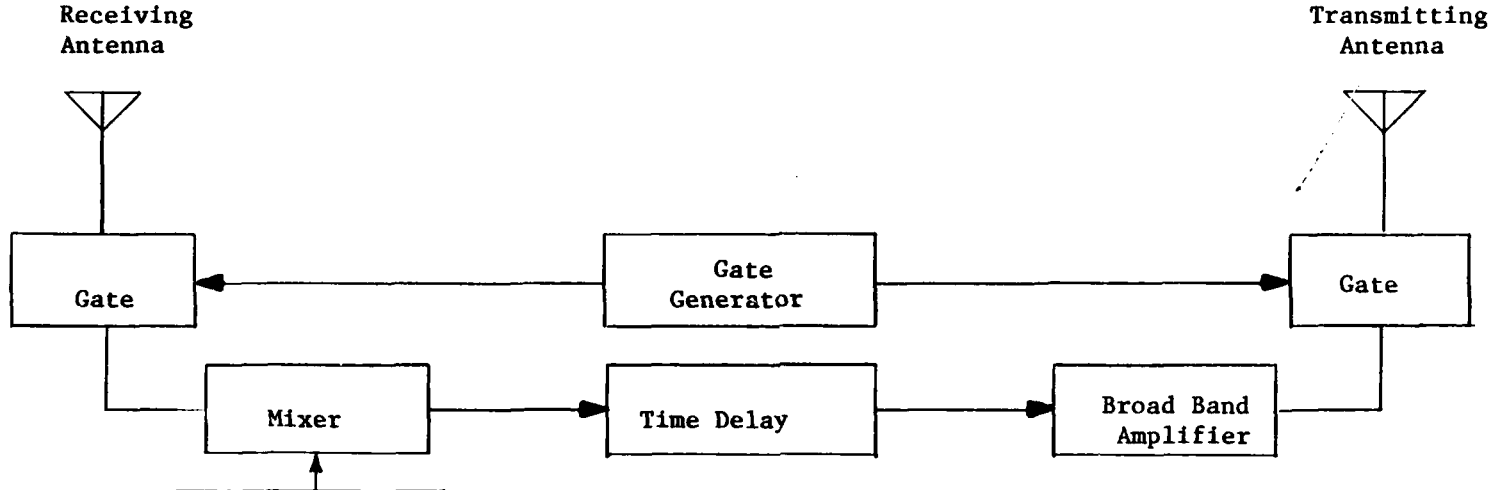


Figure 2.2.3.2 -- ECM Signal Repeaters

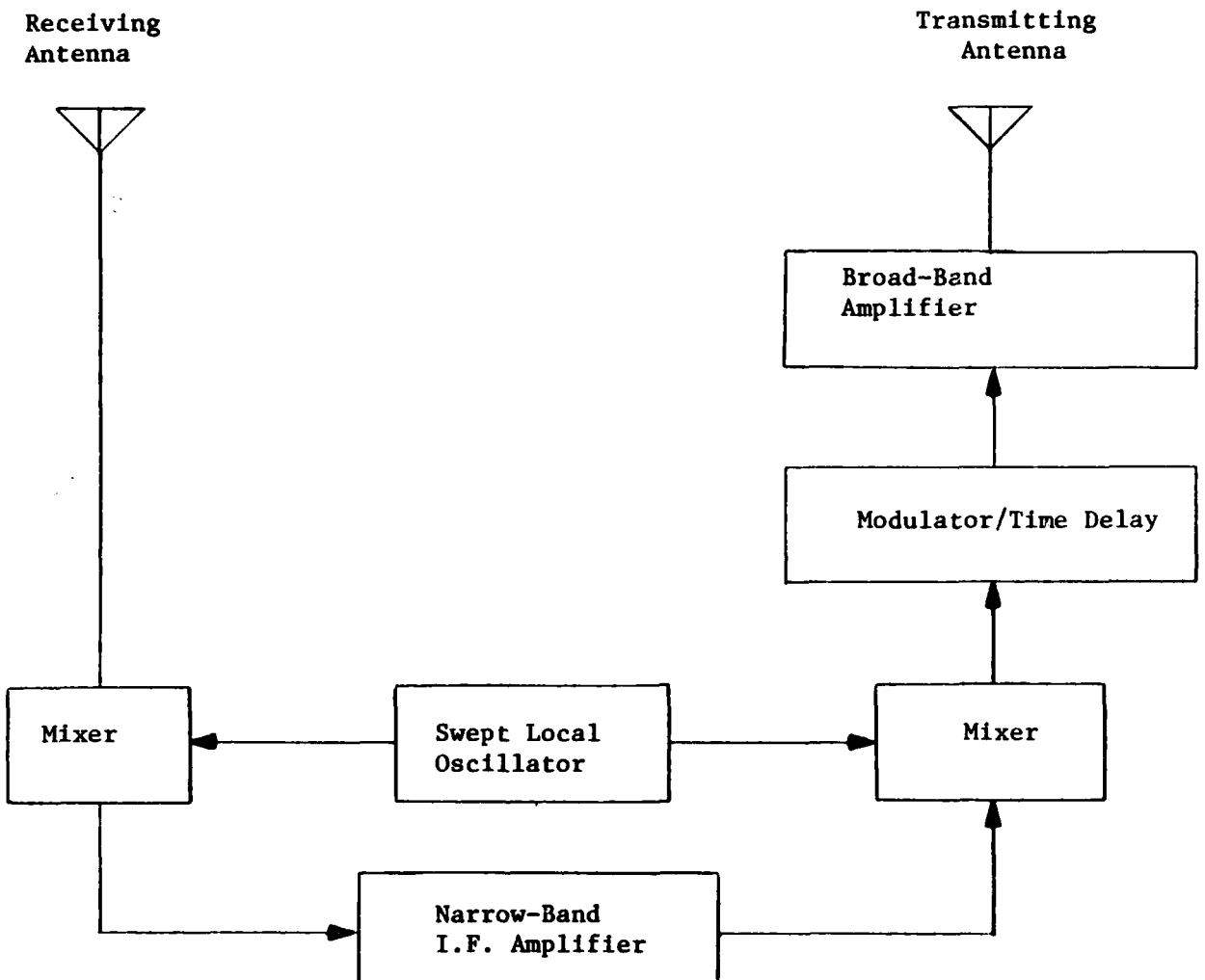


Figure 2.2.3.3 -- Swept-Frequency ECM Repeater

will be produced with the actual target (jammer) "highlighted" by an augmented return. Two techniques are employed to overcome this problem. The first is the use of an automatic gain control (AGC) in the repeater loop. The AGC tends to produce false returns of equal size (amplitude), at the same range and at different bearings (a "ring of targets"). The other technique employed to avoid "highlighting" the actual target is the use of a random gain variation in the repeater loop to produce an assymmetry in the amplitudes of the false targets. Note that these techniques will not work against scan-on-receive-only radar systems. Both techniques are depicted in the block diagram shown in Figure 2.2.3.4. The appearance of "ring of targets" deception jamming on a radar PPI display is depicted in Figure 2.2.3.5.

If it is desired to generate consistent false targets at ranges other than that of the jamming vehicle, consistent time delays or advances must be introduced into the pulse repeater loop. A time delay will produce a false target at a greater range and a time advance will produce a false target at a lesser range. A time delay always can be introduced into the transmitted pulse stream. A consistent time advance requires knowledge of the real-time pulse repetition interval. Such knowledge, in turn, implies a stable (non-time-varying) PRF for the target system signal. The time relationships of typical false target ECM pulses are shown in Figure 2.2.3.6.

If it is desired to generate consistent false targets at azimuths other than those dictated by the antenna pattern (lobes) of the target system, time delays or advances must be introduced into the repeater loop, consistent with the target system scan rate.

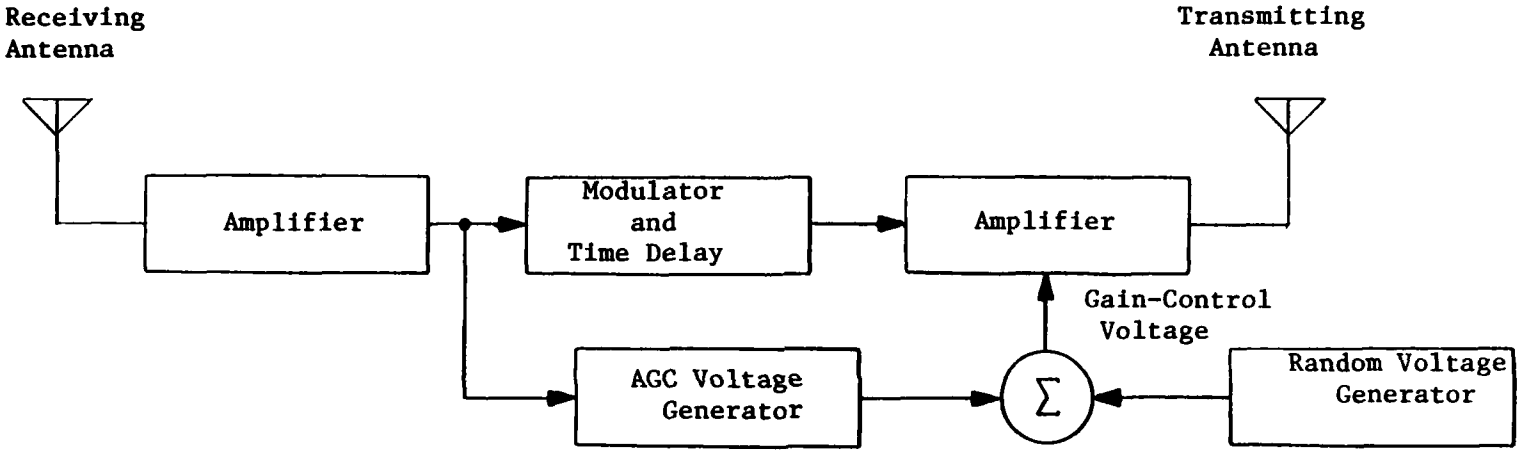
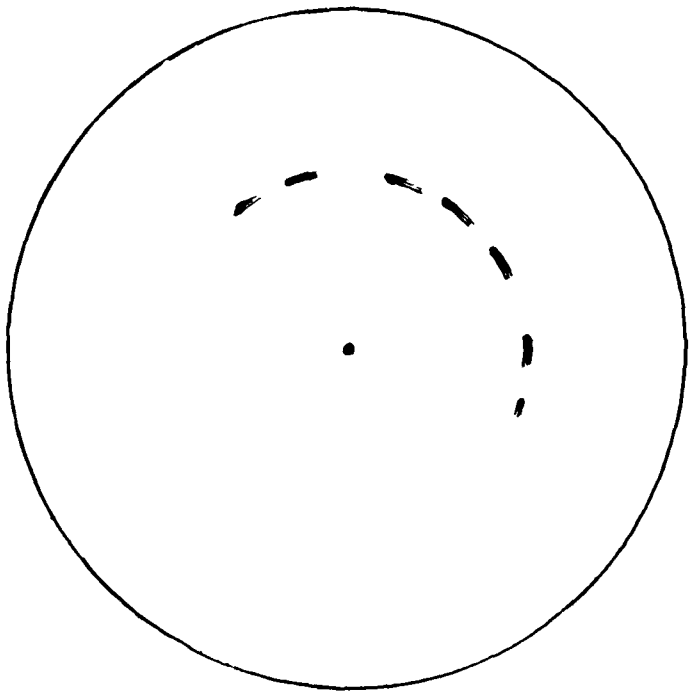
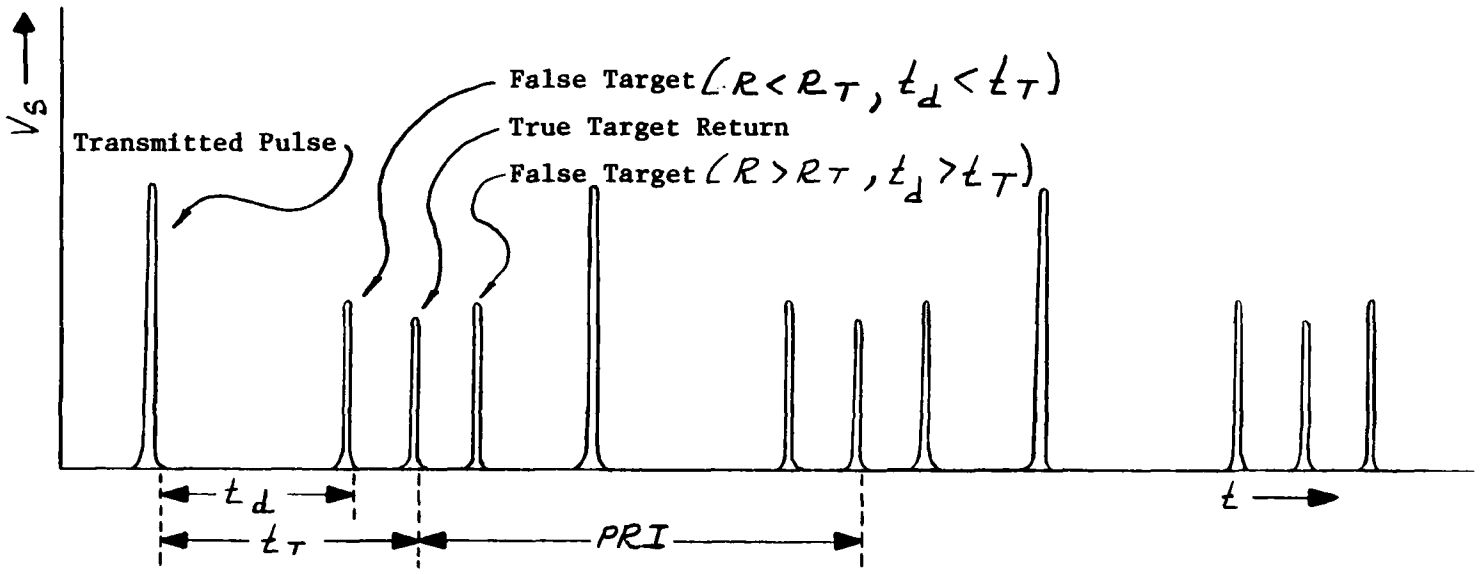


Figure 2.2.3.4 -- ECM Repeater with Automatic Gain Control and Random Gain Variation



PPI Display

Figure 2.2.3.5 -- Appearance of "Ring of Targets" Deception Jamming on Radar PPI Display



V_s = Radar Received Signal Voltage

R = Range

R_T = Range of Target

t = Time

t_d = Repeater Time Delay

t_T = Target Return Time Delay

Figure 2.2.3.6 -- ECM Pulse Repeater Returns on Radar A-Scope Display

An ECM transponder generates its own deception signal when triggered by the receipt of a signal from the target system. The essential characteristics of the received signal are preserved in the transmitted signal by properly adjusting the signal-generating equipment. The "proper" values of the signal parameters are determined by electronic reconnaissance either prior to the jamming operation or in real time (during the jamming operation). Real time adjustment of the parameters of the jamming signal requires real-time analysis of the signal to be jammed. The block diagram for an ECM transponder is shown in Figure 2.2.3.7.

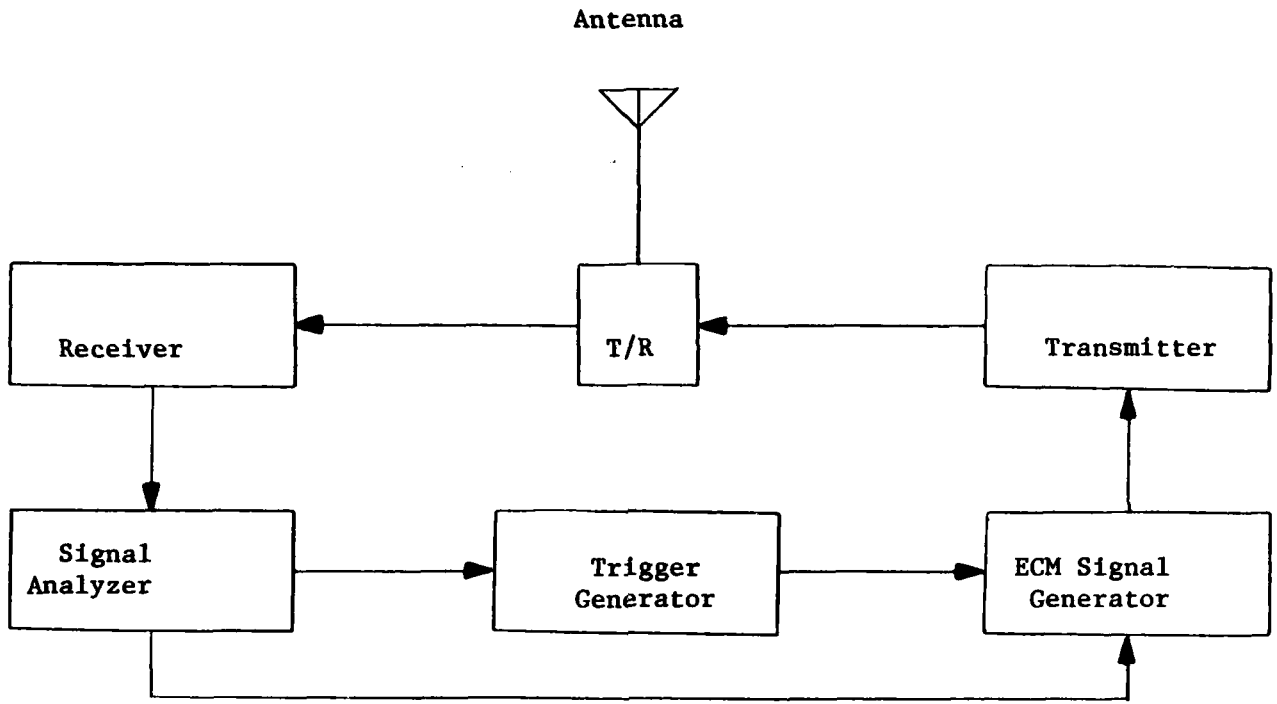


Figure 2.2.3.7 -- ECM Transponder with Real-Time Signal Analyzer

Track Breakers -- Track breakers are false-target generators with special provision for causing radar tracking loops to "break lock", or lose the target. The principal track-breaking techniques are listed below and discussed in the following paragraphs.

Range Gate Pull-Off
Velocity Gate Pull-Off
Angle Gate Deception
Inverse Gain Repeater
Scan-Rate Modulation
Cross Eye Repeater
Blinking
Skirt Jamming
Image Jamming
Cross-Polarization Jamming

It should be noted that these track-breaking techniques can be used in combination. In fact, the effectiveness of a given technique is often enhanced by the simultaneous application of a second technique.

Range Gate Pull-Off -- The range-track-breaking technique known as range gate pull-off, (RGPO), is designed to disrupt the operation of the range gate described in Section 2.17.8 of the radar text. The track breaking sequence, illustrated in Figure 2.2.3.8(a) requires a false-target generator, (such as a pulse repeater), and is given below.

(1) Place a false target return on top of (coincident in time with) the skin return from the target aircraft. (The false return must be larger in amplitude than the true return in order to "capture" the range gate.)

(2) Gradually "walk" the false return away (in time) from the true return (hopefully taking the range gate with it).

(3) Repeat steps (1) and (2).

For a self-protection jammer, an "outbound" false return is created by introducing an ever-increasing time delay in the transmitted false pulse. An inbound false return is created by decreasing the time delay from an initial value equal to one radar pulse repetition interval. This operation requires knowledge of the PRI which, in turn, requires a stable PRI.

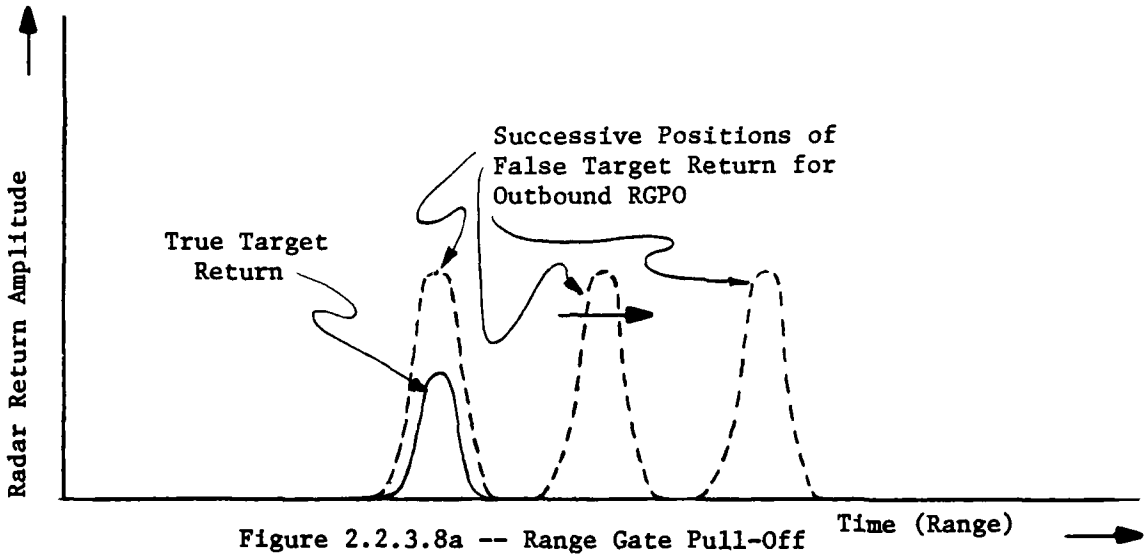


Figure 2.2.3.8a -- Range Gate Pull-Off

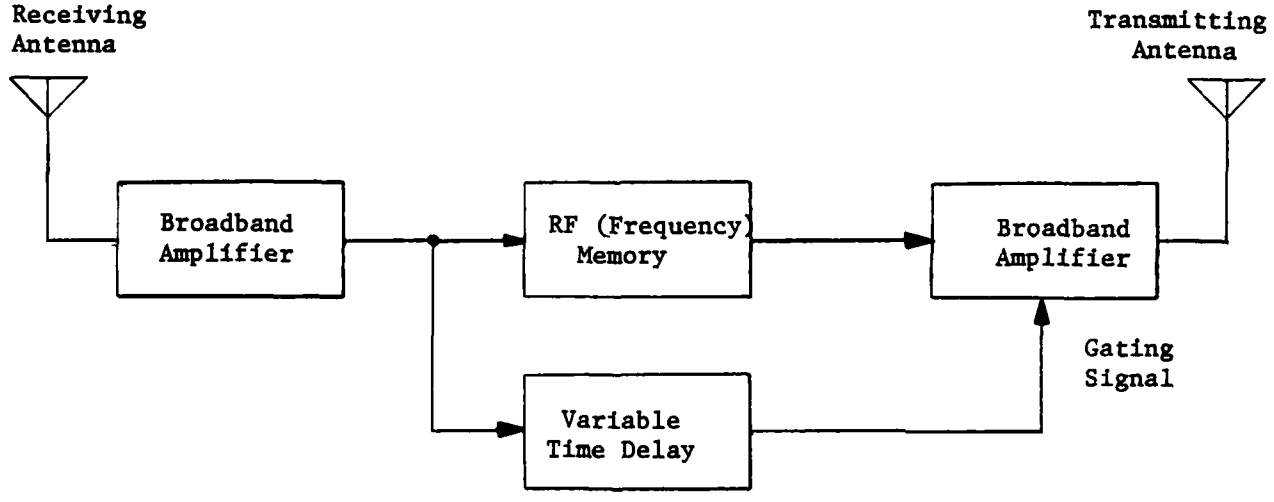


Figure 2.2.3.8b -- Range Gate Pull-Off Repeater

A simplified block diagram for a range gate pull-off repeater is shown in Figure 2.2.3.8(b). The pulse is amplified and repeated after a programmed time delay. The RF memory serves to "remember" the carrier frequency of the pulse during the delay interval.

The intent of the range gate pull-off technique is generally to cause an automatic range tracking system to break lock, thereby requiring manual operation of the tracker. Tracking errors are usually greater for manual tracking than for automatic operation.

Velocity Gate Pull-Off -- The velocity-track-breaking technique known as velocity gate pull-off (VGPO) is similar to that used for range gate pull-off and is intended to deceive the velocity gate described in Section 2.17.9 of the radar text. The tracked quantity in velocity gate pull-off is, of course, frequency (velocity) rather than time (range). (A velocity gate determines Doppler frequency shift.) Otherwise, the sequence is very similar to that for range gate pull-off. The velocity gate pull-off sequence, given below, is illustrated in Figure 2.2.3.9(a).

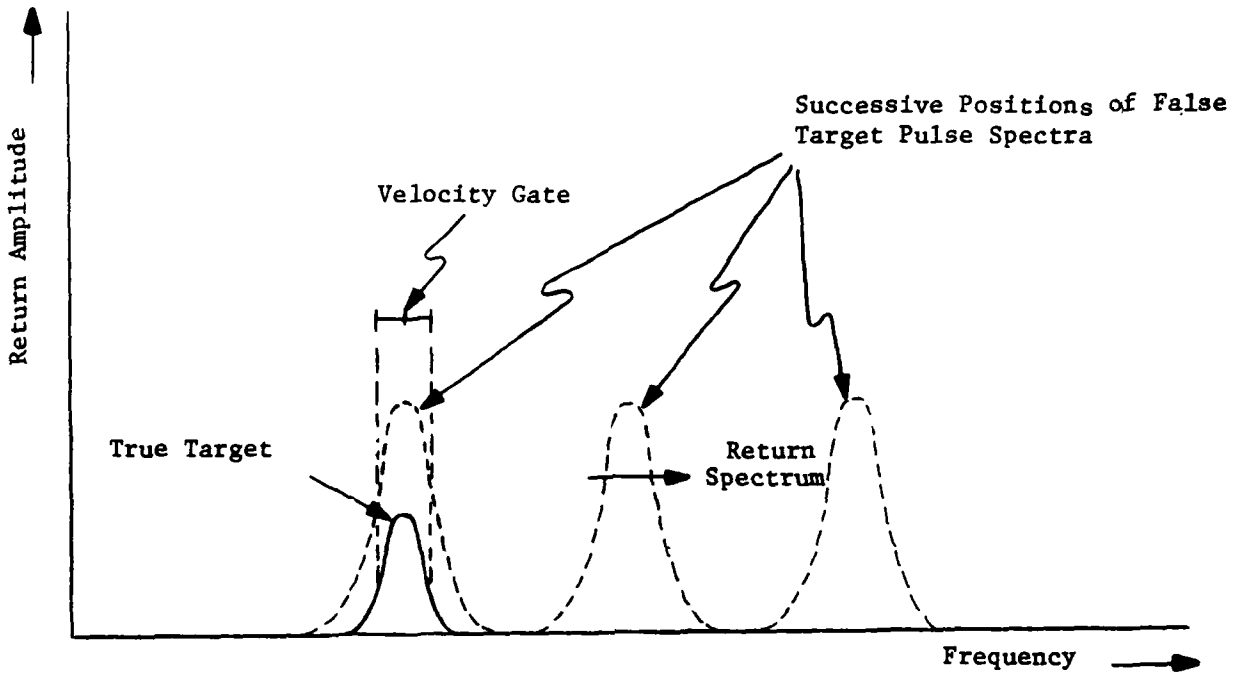
(1) Place a false target return on top of (coincident in frequency with) the skin return from the target aircraft. (The false return must be larger in amplitude than the true return in order to "capture" the velocity gate.)

(2) Gradually "walk" the false return away (in frequency) from the true return, (hopefully taking the velocity gate with it).

(3) Repeat steps (1) and (2).

A simplified block diagram for a self-protection VGPO repeater is shown in Figure 2.2.3.9(b). The received pulse is amplified, shifted in frequency as

(a) Velocity Gate Pull-Off Sequence



(b) Velocity Gate Pull-Off Block Diagram

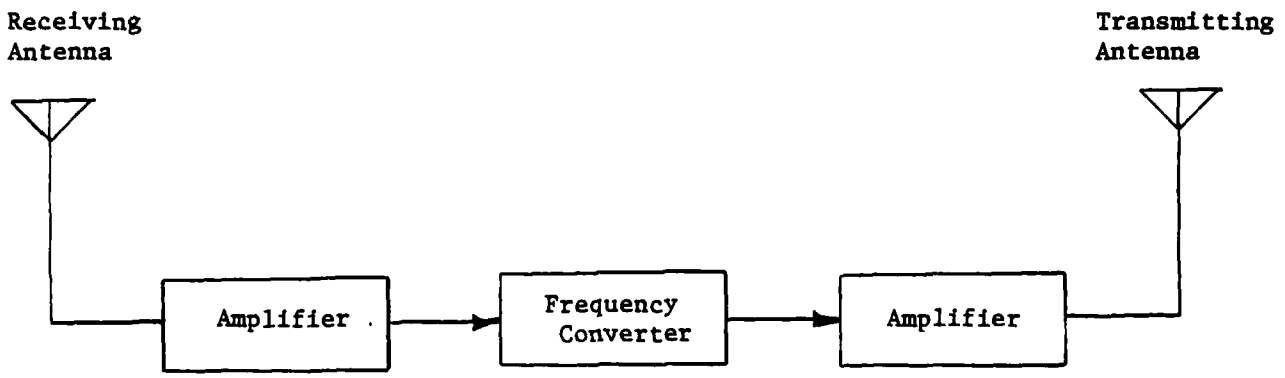
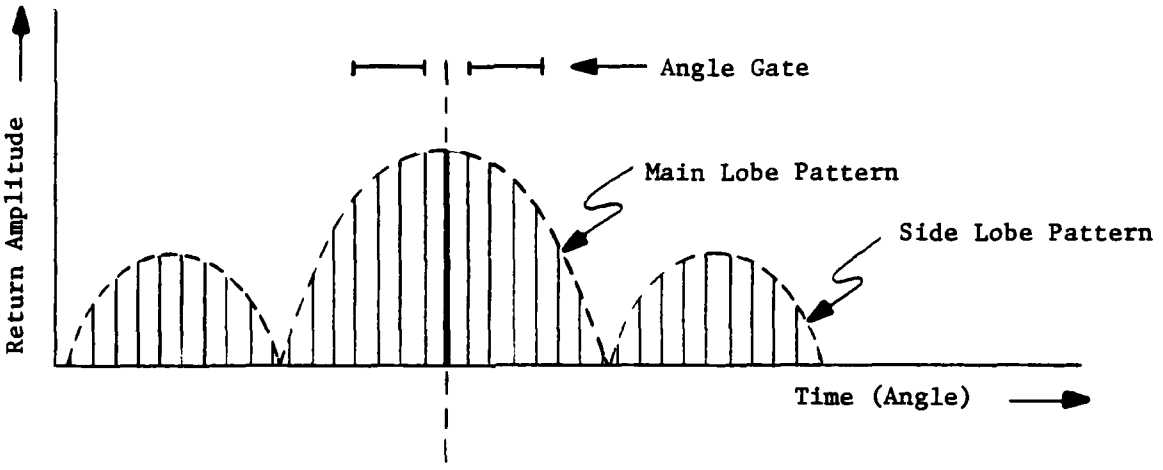


Figure 2.2.3.9 -- Velocity Gate Pull-Off

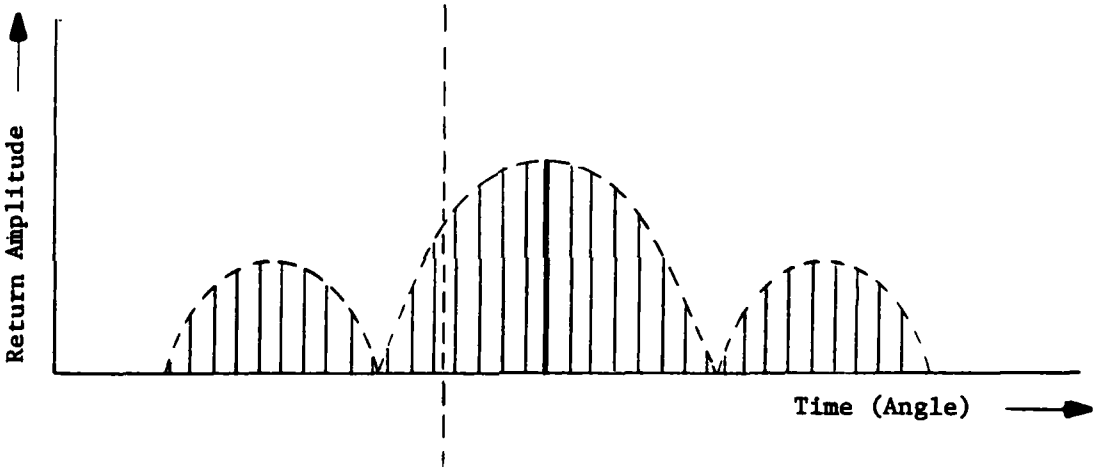
described above, and re-transmitted. The frequency converter shown in the diagram can take one of several forms, including that of a balanced mixer and that of a serrodyne modulator. The balanced mixer is a modulator (see Section 2.5.5 of the communications text) that suppresses the original carrier, thus resulting in a signal with the same modulation as that of the received signal, but with a shifted carrier frequency. The serrodyne modulator is a frequency converter that operates by introducing a time-varying phase shift into the signal.

Angle Gate Deception -- The operation of a track-while-scan angle-tracking gate is described in Section 2.17.10 of the radar text. The angle gate deception technique described here is designed to introduce errors into such an angle tracking system. In Figure 2.2.3.10(a) is shown the target return amplitude pattern produced at the radar receiver when a scanning radar scans a target. A similar pattern is produced at the target as the radar scans. The pattern, therefore, can be received, delayed, and retransmitted by the ECM receiver, producing, at the radar receiver, the amplitude pattern shown in Figure 2.2.3.10(b). The total pattern seen by the radar is, thus, that shown in Figure 2.2.3.10(c). As can be seen, the apparent main-lobe peak has been shifted carrying the angle gate with it. Note that the necessary time delay is greater than one pulse repetition interval. The block diagram for an angle-deception repeater is shown in Figure 2.2.3.11. The received pulse train (modulated by the scanning antenna pattern as shown in Figure 2.2.3.10(a)), is received and detected. The detected scan pattern envelope is then used to generate a suitably synchronized and delayed ECM signal envelope. This envelope is impressed upon the received pulse train and the resulting modulated ECM signal, shown in Figure 2.2.3.10(b), is transmitted.

(a) Target Return Pattern at Receiver



(b) ECM Repeater Signal Pattern at Receiver



(c) Combined Signal Pattern at Receiver

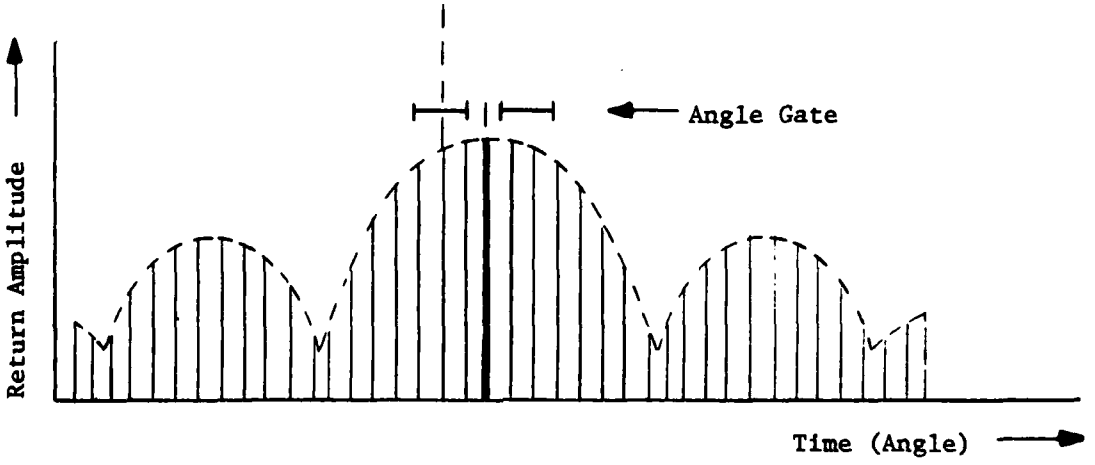


Figure 2.2.3.10 -- Angle Gate Deception

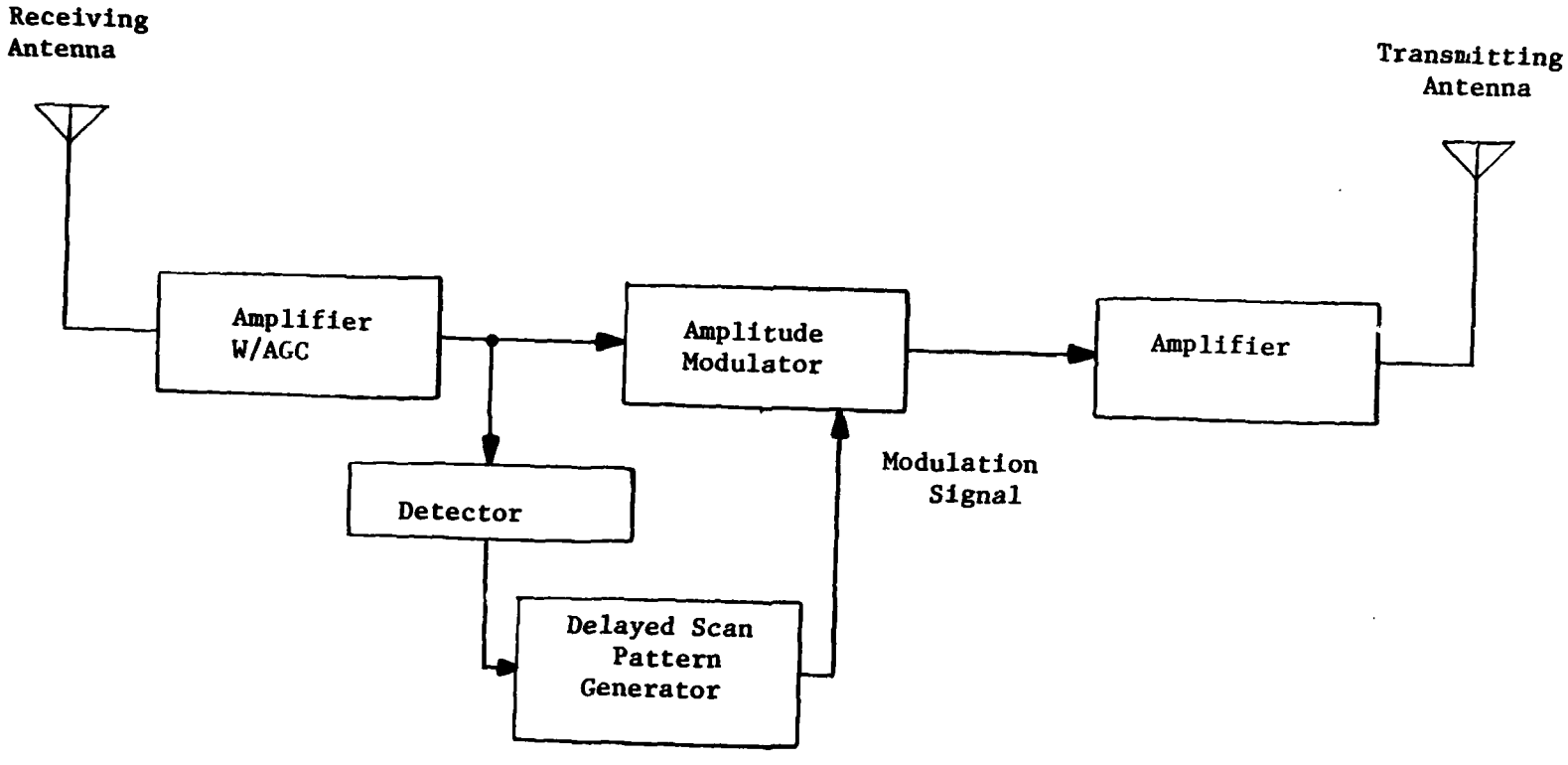


Figure 2.2.3.11 -- Angle Gate Deception Repeater

The Inverse-Gain Repeater -- Another type of angle tracker deception is achieved by the inverse-gain repeater shown in Figure 2.2.3.12. The received signal is re-transmitted after being amplified by an amplifier the gain of which is varied inversely with respect to the amplitude of the received signal. Theoretically, the amplifier gain can be controlled so as to produce, at the radar receiver, an apparent target return signal unmodulated by the antenna beam pattern. While such a return would deny all angle information to the radar, in practice it is very difficult to set the absolute level of the gain to the required value. For that reason, an alternate method is generally employed. That is, a high inverse gain is used with a threshold (cut-off) level set so as to produce on-off operation of the repeater. The result is the repeater signal shown in Figure 2.2.3.13(b). The combined (target plus jammer) signal at the radar receiver is shown in Figure 2.2.3.13(c). As shown therein, the signal envelope pattern is essentially inverted, thus providing a tracking error signal 180° out of phase from the true target signal.

Scan-Rate Modulation -- When the scan-modulation pattern is not detectable at the target, (as, for example, with a scan-on-receive-only radar), the jamming signal can be amplitude modulated at a frequency equal to that of the antenna scan, producing a pattern-distorting effect similar to that of the angle gate deception techniques already discussed. When the precise scan frequency is unknown, a swept envelope modulation frequency can be employed. Sweeping the modulation frequency produces intermittent disruption of the radar angle tracker as the swept frequency passes through the actual antenna scan frequency. A simplified block diagram for a scan-rate modulation angle deception repeater is shown in Figure 2.2.3.14.

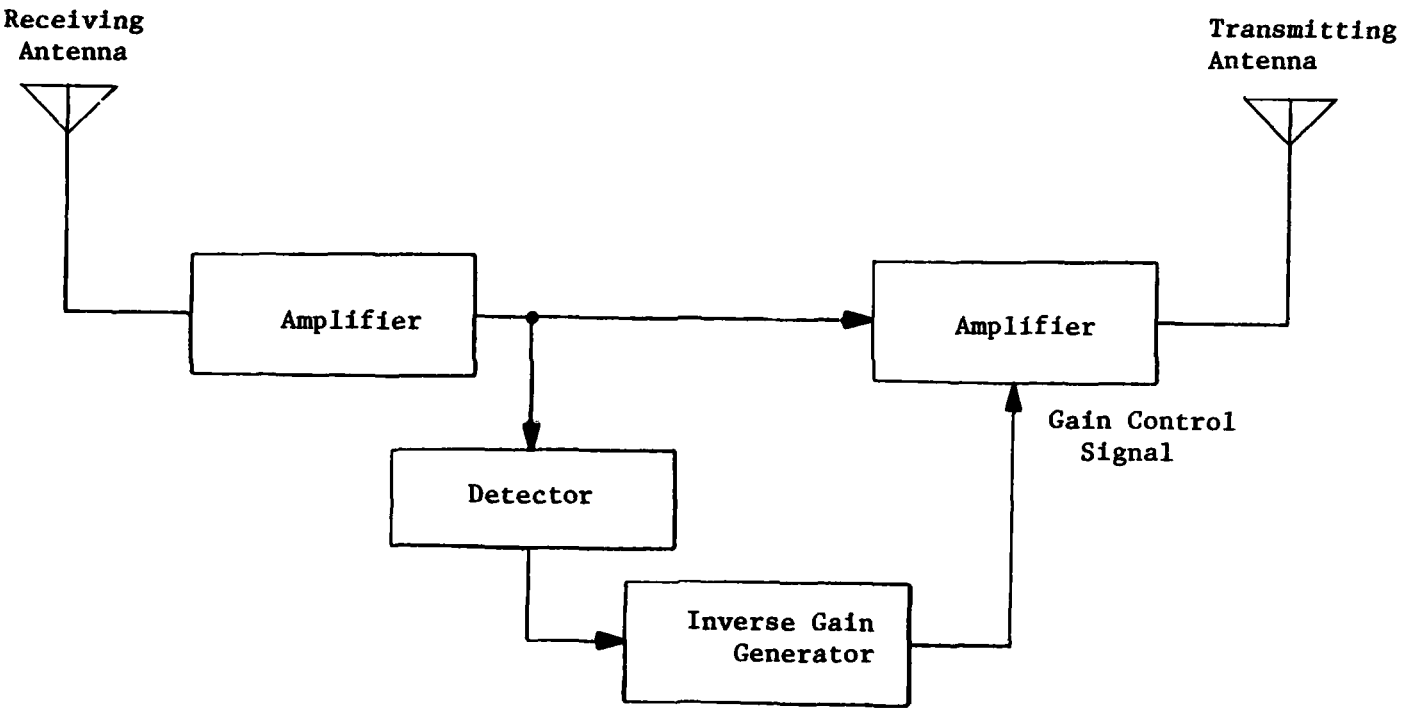


Figure 2.2.3.12 -- Inverse Gain Repeater

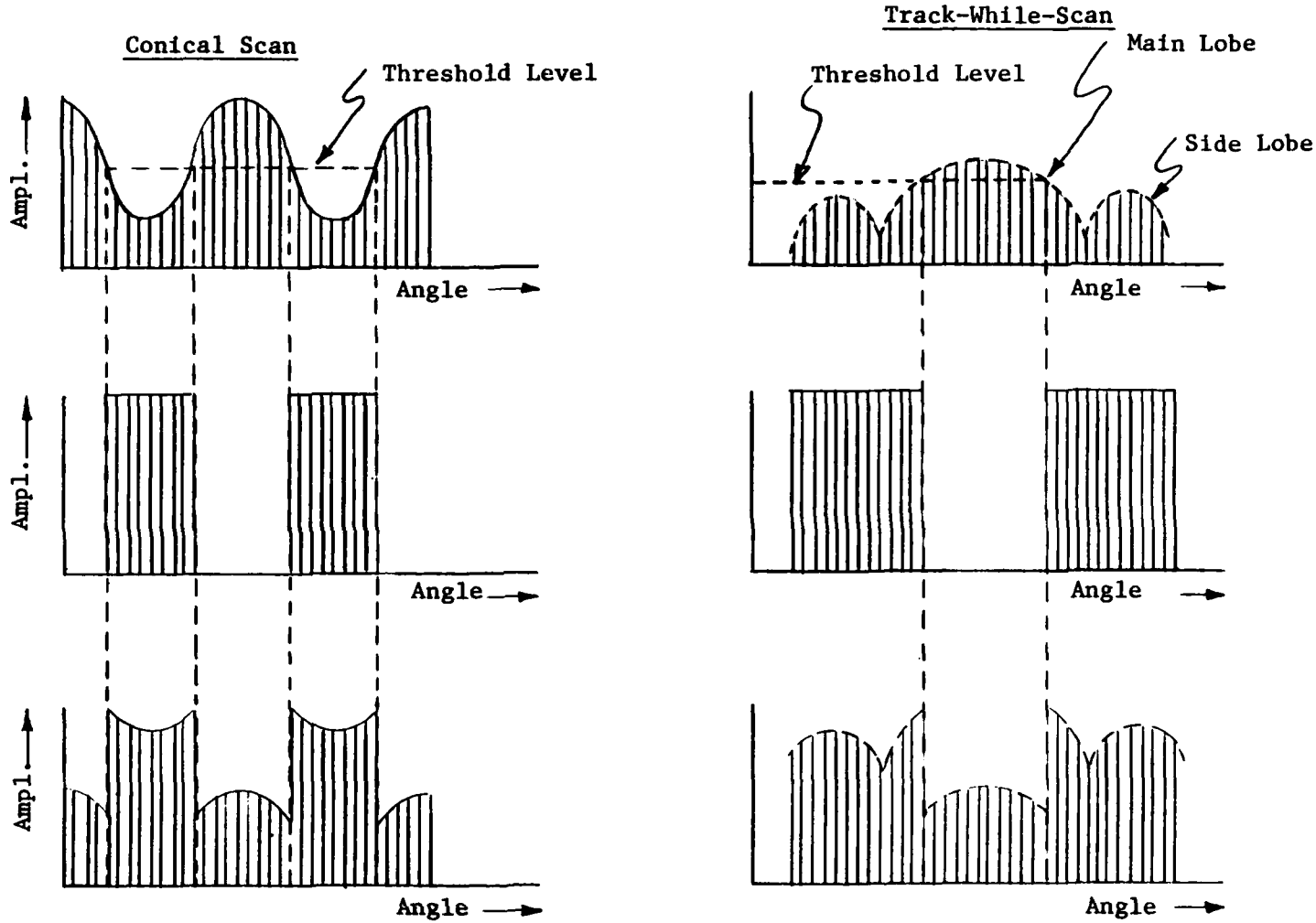


Figure 2.2.3.13 -- Inverse Gain Repeater ECM

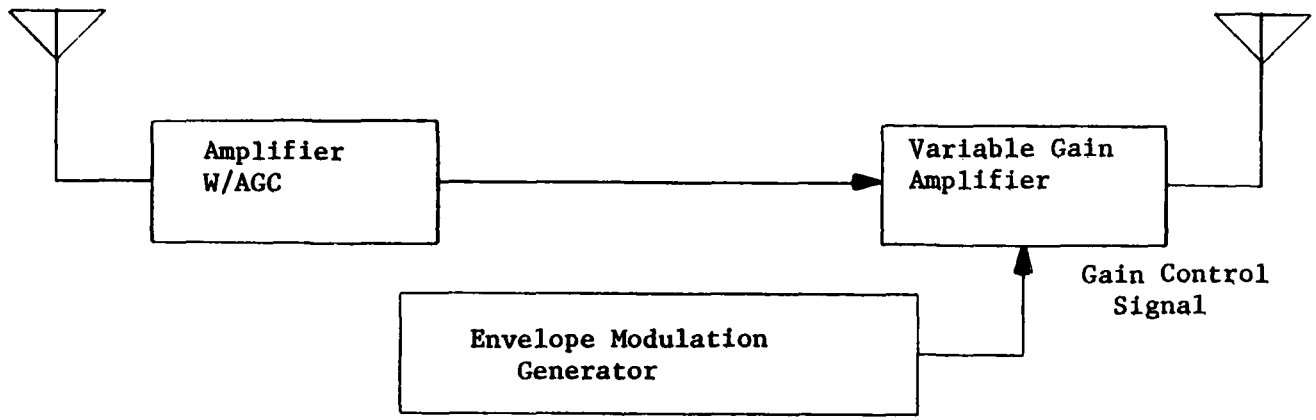


Figure 2.2.3.14 -- Scan Rate Modulation Repeater

Cross Eye Repeater -- As discussed in Section 2.3.5 of the radar text, an interferometer radar derives target angular position information from the difference in phase between target returns received at two antennas. Because this angular determination is not dependent on time or antenna pattern, it is very difficult to jam. One method effective against an interferometer radar is known as Cross Eye. Cross Eye is a dual-channel repeater designed to produce an interferometer field pattern with abrupt changes in phase as a function of aspect angle. A dual-channel repeater is shown in Figure 2.2.3.15. The equi-phase wavefront (loci of equal phase) produced by a two-source interferometer is shown in Figure 2.2.3.16. A phase monopulse (interferometer) radar tracking the sources would attempt to align its boresight perpendicular to the wavefront. Because of the dual-repeater operation of Cross Eye, the wavefront pattern is always oriented so as to place the victim radar at a point of rapidly changing phase.

Cross Eye can be considered a method of systematically inducing a phenomenon known as "glint" whereby reflections from two radar targets (or two reflecting surfaces on a single target) mutually interfere, producing scintillations or fluctuations in phase angle with time and aspect angle. Another method of inducing such phase fluctuations is Formation Jamming and consists simply of maintaining two or more aircraft in close proximity (formation) so as to induce "glint" in the radar returns.

Blinking Jammers -- Angle tracking loop jamming can sometimes be achieved by employing two jammers, pulsed alternately. The two jammers must be separated in angle, but simultaneously in the radar instantaneous field of view and, if range and velocity gates are employed, they must be in the same range and velocity

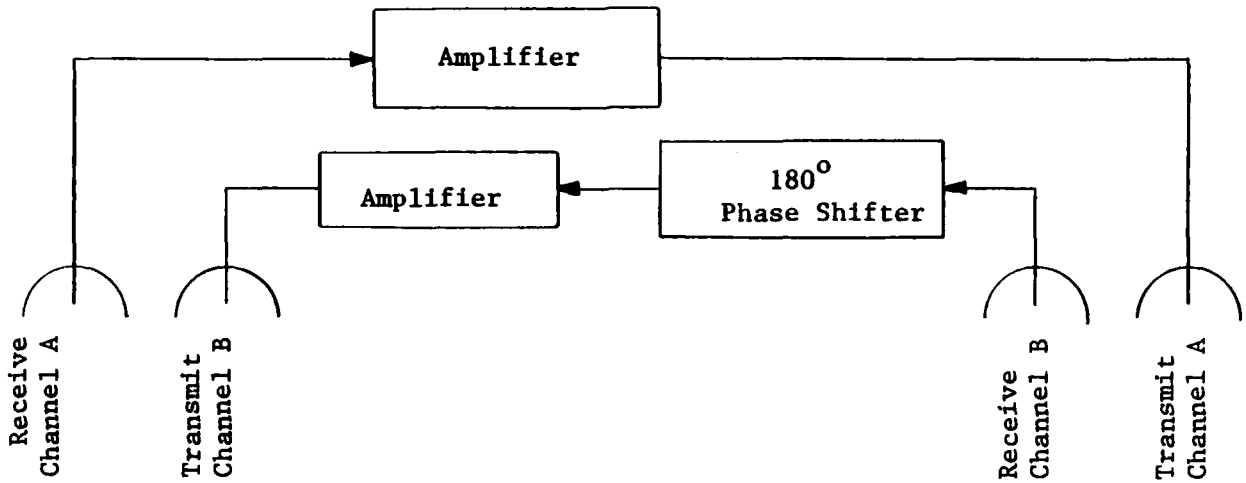


Figure 2.2.3.15 -- Cross Eye Repeater Block Diagram

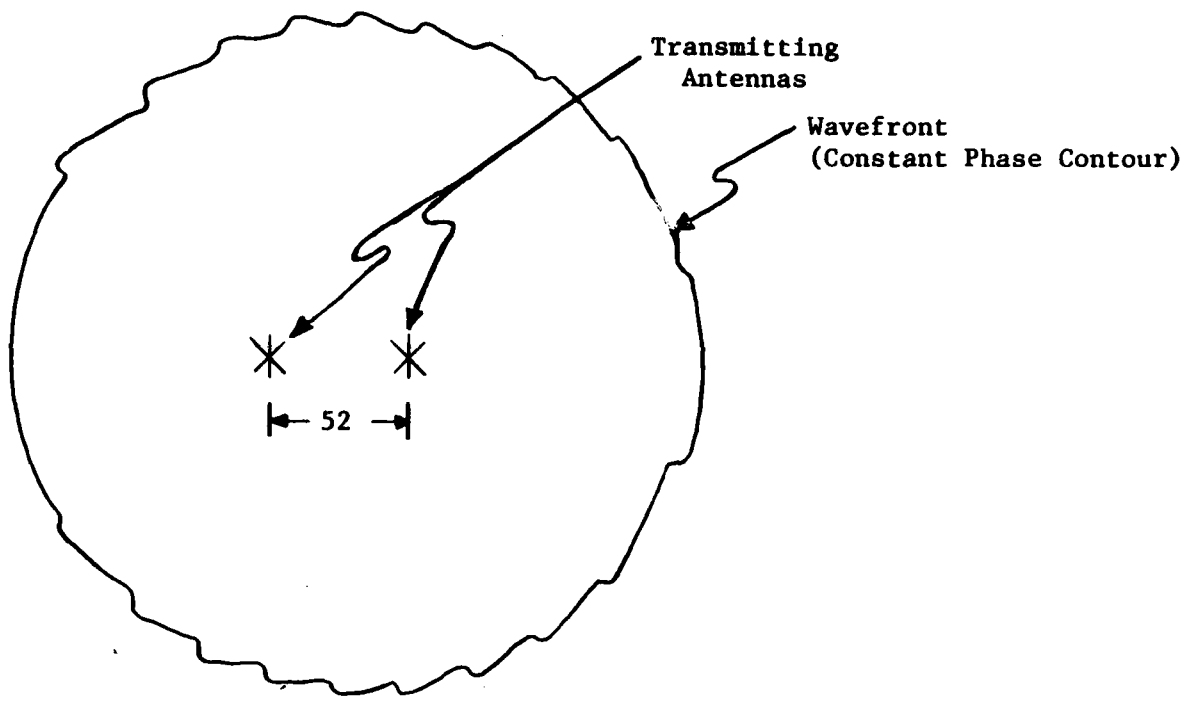


Figure 2.2.3.16 -- Cross Eye Interfereometer Wavefront

"bins". The effect of alternate operation (blinking) is to cause dynamic transients in the angle tracking loop, hopefully sufficient to cause loss of the targets.

Cross-Polarization Jamming -- A monopulse angle tracking radar can sometimes be jammed by an ECM signal polarized at right angles to the radars radiation.

Skirt and Image Frequency Jamming -- A monopulse radar without adequate RF tuning can sometimes be jammed by an ECM signal slightly detuned from the radar carrier frequency.

Missile Proximity Fuse Jamming -- The principal types of missile proximity fuses are listed below.

Super-Regenerative
Range
Velocity
Multi-mode

The super-regenerative fuse utilizes an oscillatory circuit with positive (regenerative) feedback created by reflections from a target back to a radiating antenna. The feedback from a target increases as the target approaches, triggering the fuse when the oscillations reach a set level. A super-regenerative fuse can be prematurely detonated by an ECM repeater.

A range fuse is a miniature ranging radar. The fuse is triggered when the range goes below a set value. Such a fuse can be detonated by one of the range-deception techniques previously discussed. The deception range must be less than the actual range.

A velocity fuse measures target-to-missile relative radial velocity by detecting the Doppler shift or by determining the time rate-of-change of range. At the point of closest approach, the relative radial velocity goes to zero. Velocity fuses are triggered when that velocity drops below a set value. Such fuses can be prematurely detonated by one of the velocity deception techniques previously discussed.

Multi-mode fuses use two or more triggering criteria. Some fuses employ both range and velocity. Others determine velocity by both the Doppler shift and range rate-of-change. In either case, the ECM signals must be consistent for successful deception. The most reliable anti-missile-fuse ECM is often the use of a decoy with appropriate cross-section augmentation. Such decoys can also employ active jammers and also infrared sources for use against heat-seeking missiles.

Missile Guidance Up-Link Jamming -- Missile guidance up-link jamming is generally difficult because of the unfavorable look angle from an airborne jammer to the missile guidance receiver antenna which is pointed down at the guidance station. This problem is only partly offset by the fact that, as the missile-to-target range decreases, the jamming signal becomes more effective.

2.2.4 Jam-to-Signal Ratio -- The effectiveness of jamming is primarily determined by the ratio of the jamming power to the (target return) signal power, at the radar. This ratio, (J/S), is a function of the sensor characteristics, the jammer characteristics, and the ranges between target and radar and jammer and radar.

For the general case (stand-off jamming) where the target and the jammer are not co-located, the (target return) signal power, S, and the jammer power, J, and the jam-to-signal power ratio, J/R, into the radar receiver, are given by the following equations. (Refer to Section 2.4 of the radar text for a development of the radar range equation.)

$$S = \frac{P_R G_{RT}^2 \sigma \lambda^2}{(4\pi)^3 R_{RT}^4} \quad \text{(Watts)} \qquad [2.2.4.1]$$

$$J = \frac{P_J G_{JR} G_{RJ} \lambda^2}{(4\pi)^2 R_{JR}^2} \quad \text{(Watts)} \qquad [2.2.4.2]$$

$$J/S = \frac{4\pi P_J G_{JR} G_{RJ} R_{RT}^4}{P_R G_{RT}^2 \sigma R_{JR}^2} \quad \text{(N.D.)} \qquad [2.2.4.3]$$

where:

G_{JR} = Gain of jammer antenna in direction of radar.

G_{RJ} = Gain of radar antenna in direction of jammer.

G_{RT} = Gain of radar antenna in direction of target.

J/S = Jam-to-signal power ratio at radar receiver.

P_J = Power of jammer within bandwidth of radar receiver.

P_R = Power of radar.

λ = Wavelength of signal.

σ = Target radar cross section.

R = Range

For the case where the target and jammer are essentially co-located, as with self-protection jamming, the target return signal power, jamming power, and jam-to-signal ratio into the radar receiver, are given by the following equations.

$$S = \frac{P_R G_{RT}^2 \sigma \lambda^2}{(4\pi)^3 R_R^4} \quad \text{(Watts)} \qquad [2.2.4.4]$$

$$J = \frac{P_J G_{JR} G_{RT} \lambda^2}{(4\pi)^2 R_{RT}^2} \quad \text{(Watts)} \qquad [2.2.4.5]$$

$$J/S = \frac{4\pi P_J G_{JR} R_{RT}^2}{P_R G_{RT} \sigma} \quad \text{(N.D.)} \qquad [2.2.4.6]$$

2.2.5 Burn-Through Range -- At radar-to-target ranges less than some minimum value, the target will be detectable despite the jamming signal. This minimum effective jamming range, called burn-through range, $R_{B/T}$, can be derived from equations 2.2.4.3 and 2.2.4.6 by setting J/S equal to the maximum value for which the target is detectable, (J/S) Max., and solving for range.

For stand-off jamming, the burn-through range is given by:

$$R_{B/T} = \left[\frac{P_R G_{RT}^2 \sigma R_{JR}^2 (J/S)_{Max.}}{4\pi P_J G_{JR} G_{RJ}} \right]^{1/4} \quad \text{(Meters)} \qquad [2.2.5.1]$$

For self-protection or escort jamming, the burn-through range is given by:

$$R_{B/T} = \left[\frac{P_R G_{RT} \sigma (J/S)_{Max.}}{4\pi P_J G_{JR}} \right]^{1/2} \quad \text{(Meters)} \qquad [2.2.5.2]$$

2.2.6 Repeater Gain -- In most applications, the jamming power, P_{JE}, emitted by a repeater is not constant, but is proportional to the received radar signal at the jammer. That is:

$$P_{JE} = G_e \, P_{RJ} \qquad \text{(Watts)} \qquad [2.2.6.1]$$

where P_{RJ} is the radar signal power into the jammer receiver and G_e is the internal (electronic) gain of the jammer repeater. Thus, for self-protection jamming, the jammer power into the radar receiver, J, is given by:

$$J = \frac{P_{JE} \, G_{JR} \, G_{RT} \, \lambda^2}{(4\pi)^2 \, R_{RT}^2} \qquad \text{(Watts)} \qquad [2.2.6.2]$$

or:

$$J = \frac{P_R \, G_{RT}^2 \, G_{JR}^2 \, G_e \, \lambda^4}{(4\pi)^4 \, R_{RT}^4} \qquad \text{(Watts)} \qquad [2.2.6.3]$$

From Equation [2.2.4.4], the target return signal power into the radar receiver is given by:

$$S = \frac{P_R \, G_{RT}^2 \, \sigma \, \lambda^2}{(4\pi)^3 \, R_{RT}^4} \qquad \text{(Watts)} \qquad [2.2.6.4]$$

The jam-to-signal power ratio into the radar receiver is, then, given by:

$$J/S = \frac{G_{JR}^2 \, G_e \, \lambda^2}{4\pi \, \sigma} \qquad \text{(N.D.)} \qquad [2.2.6.5]$$

Equating J/S with the maximum value for which the radar is able to detect the target through the jamming, (J/S) Max., and solving for the required jamming repeater electronic gain, G_e, we have:

$$G_e = \frac{4\pi\sigma\,(J/S)_{Max.}}{G_{JR}^2\,\lambda^2} \qquad \text{(N.D.)} \qquad [2.2.6.6]$$

Equation [2.2.6.6] assumes that the bandwidth of the repeater signal is the same as that of the radar signal. If the repeater modulates the signal before re-transmitting it, thereby increasing the repeated signal bandwidth so that only a fraction 1/k of the repeater power is within the radar receiver bandwidth, then Equation [2.2.6.6] must be modified by inserting a factor k into the numerator.

For a repeater gain G_e given by Equation [2.2.6.6], the power from the jammer is given by Equation [2.2.6.1]. That is:

$$P_{JE} = \frac{P_R\,G_{RT}\,\sigma\,(J/S)_{Max.}}{4\pi\,G_{JR}\,R_{RT}^2} \qquad \text{(Watts)} \qquad [2.2.6.7]$$

If, in Equation [2.2.6.7], R_{RT} is set equal to the minimum range for which the jammer must be effective, P_{JE} will be equal to the required maximum jammer power. The burn-through range is, then, given by:

$$R_{B/T} = \left[\frac{G_{RT}\,(J/S)_{Max}\,P_R}{4\pi\sigma\,G_{JR}\,P_{JE}}\right]^{1/2} \qquad \text{(Meters)}$$

2.3 Electronic Counter-Countermeasures

2.3.1 The Nature of ECCM -- As previously indicated, ECCM is that branch of electronic warfare concerned with preventing the electronic countermeasures of the adversary from interfering with the operation of "communications" equipment employed by friendly forces. The rapid evolution characteristic of electronic warfare makes it imperative for the designer to build into his equipment maximum resistance to interfering signals in general, to respond rapidly to new ECM practices employed by the adversary, and, when possible, to anticipate future ECM developments. Rapid response to ECM practices and anticipation of future ECM developments depend greatly on effective electronic reconnaissance (ER). Designing equipment for maximum resistance to interference is not unique to the field of electronic warfare. Intentional jamming signals often bear a resemblance to noise arising from natural causes. Designing a system to maximize the signal-to-noise ratio, (S/N), will generally result in a system with a natural resistance to jamming.

ECCM provisions are of two basic kinds: hardware implementations and operational techniques. The hardware implementations are, of course, "built in" and depend upon the system design and the specific ECM being countered. While provision for some ECCM operational techniques also must be "built in", such techniques generally offer the important advantage that they can be modified in the field. This advantage is often decisive and requires a knowledgeable and, generally, a dedicated operator.

2.3.2 The objectives of ECCM -- Electronic counter-countermeasures are intended to accomplish one or more of the seven basic objectives listed below and discussed in the following paragraphs. Examples of specific radar ECCM techniques are listed by category in Section 2.3.3 of this text.

Deny Jamming Information to Adversary
Avoid Jamming Signal
Increase Effective Signal Power
Reject False Information (Deception Jamming)
Prevent Receiver Saturation (Noise Jamming)
Prevent System Saturation
Maintain Signal Tracking

Denial of Jamming Information to Adversary -- Effective ECM, even noise jamming, requires knowledge of the system to be jammed. The ideal ECCM is denial to the adversary of knowledge of even the existence of the system to be protected. Failing that ideal, ECCM should, at least, deny to him a knowledge of the parameters of the system.

Avoidance of Jamming Signal -- The avoidance of ECM implies the ability to elect alternate modes of operation. A system can elude the jammer in the time domain, (e.g. intermittent operation), the space domain, (e.g. antenna blanking), or the parameter domain, (e.g. frequency, PRF, or polarization discrimination). Diversity in system parameters and modes of operation is an essential ECCM practice.

Increase of Signal-to-Jamming Ratio -- The information signal-to-jamming signal power ratio, (S/J), can be increased by: (1) increasing the level of the true signal received by the system, (e.g. increased transmitter power); (2) reducing the level of the jamming signal received by the system, (e.g. directive antennas),

or (3) discriminating, within the system, between signal and jamming, (e.g. correlation detection).

Rejection of False Information -- Rejection of false information requires a means of discriminating between the true (information) signal and a false (deception jamming) signal. Such discrimination can be based upon a natural characteristic of the true signal, (e.g. frequency or pulse width); a peculiar characteristic of the deception signal, (e.g. angle of arrival); or a special characteristic of the information signal imparted by the system, (e.g. signal coding).

Prevention of Receiver Saturation -- Often the objective of noise jamming is to drive the receiver into saturation (overload). Driving the receiver into saturation not only obscures the information signal but produces recovery transients that further disrupt the system. Receiver saturation can be prevented by reducing the response of the receiver to large-amplitude signals (e.g. logarithmic amplification or limiting).

Prevention of System Saturation -- System saturation is caused by the existence of too high a data rate for the system to handle (for example, too many apparent targets for a radar to track simultaneously. System saturation can be prevented by reducing the amount of information accepted by the system (e.g. threshold sensitivity control).

Maintenance of Signal Tracking -- Signal tracking is the process of signal recognition by means of the continuity observed in some signal characteristic. An example of signal tracking is the use of predictive tracking in radar, based

upon target position and/or velocity continuity. Continuing recognition (tracking) of a communication signal can be greatly enhanced by signal coherence or direct sequence coding.

2.3.3 ECCM Technique Definitions -- The major ECCM techniques are listed below and discussed in the following paragraphs.

Transmitter/Antenna ECCM Techniques

Adaptive Antenna
Angular Resolution Improvement
Antenna Gain Increase
Bistatic Antennas
Frequency Diversity
Low Scan Rate Antenna
Mainlobe Blanking
Monopulse Detection
Polarization Diversity
Power Increase
PRF Diversity
PRF Increase
Scan Diversity
Scan-on-Receive-Only
Scan Rate Diversity
Sidelobe Cancellation
Sidelobe Reduction
Spread-Spectrum Modulation

Receiver/Signal Processor ECCM Techniques

Coherent Signal Processing
Correlation Detection
Double Threshold Detection
Dynamic Range Increase
Gain Control
Leading-Edge Tracking
Linearity Improvement
Logarithmic Amplification
Moving Target Detection
Noise and Jamming Cancellation
Pre-Detection Frequency Discrimination
Predictive Tracking
Pulse Discrimination
Pulse Integration
Range Gating
Range Resolution Improvement
Shielding
Target Return Width Discrimination
Threshold Detection
Velocity Gating
Wideband Limiting (Dicke Fix)
Zero-Crossing Detection

Data Processing/Operational Technique ECCM Techniques

Anti-Arm ECM
Aural Detection
Decoy Radiators
Doppler/Range Rate Comparison
Electronic Reconnaissance
Human Operator Monitoring and Control
Home-on-Jam Missile
Manually-Aided Tracking
Missile Fuse ECCM (Delayed Arming)
Multiple-Sensor Tracking (Netting)
Operating-Time Minimization
Remote Location of Antenna
Sensor Mobility
Threat Identification
Tracking Acceleration Limiting
Tracking-on-Jamming Signal
Triangulation

Transmitter/Antenna ECCM Techniques

Adaptive Antenna -- An adaptive ECCM antenna determines the direction to a jamming source and adjusts its receiving pattern to place a null in that direction. Such antennas require multiple radiators (an interferometer array) and can be entirely automated.

Angular Resolution Improvement -- By improving the angular resolution (narrowing the effective beamwidth) of a receiving antenna, it often is possible to reject a jamming signal even when it originates from a source close to the desired signal source in bearing (angle).

Antenna Gain Increase -- The information signal, (and hence the signal-to-jamming ratio), can be increased by increasing the effective radiated power (ERP) of the transmitter/antenna. One method of increasing the ERP is to employ a high-gain antenna.

Bistatic Antennas -- By physically separating the transmitting and receiving antennas, a system can protect the receiving antenna from jamming aimed at the transmitting antenna. (Directive jamming systems generally aim their signal at the source of radiation to be jammed.)

Frequency Diversity -- Frequency diversity, the capability of changing carrier frequency or using multiple frequencies, allows the system to: (1) deny jamming information to the adversary, (2) avoid the jamming signal in the frequency domain, or (3) discriminate against the jamming signal on the basis of frequency. Frequency

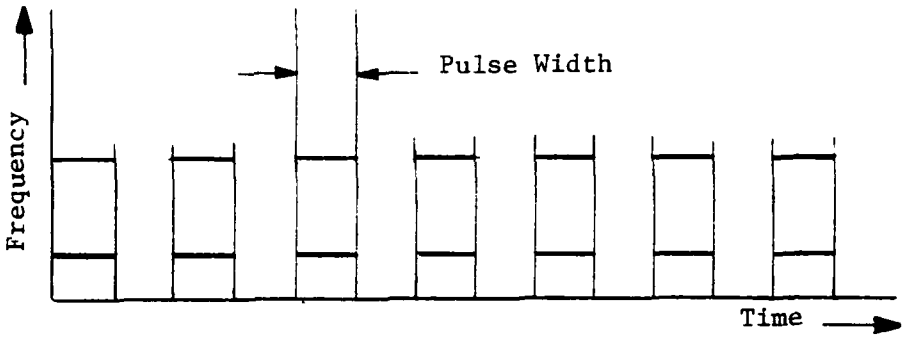
diversity is implemented by the four methods illustrated in Figure 2.3.3.1. In a multiple-frequency system, two or more frequencies are simultaneously employed as shown in part (a) of the figure. In a fast-tuning system, the frequency is changed between groups of pulses as shown in part (b) of the figure. In frequency-agile systems, the frequency is changed pulse-to-pulse as shown in part (c) of the figure. In intra-pulse FM systems, the frequency is changed within the pulse as shown in part (d) of the figure.

Low Scan Rate Antenna -- When target return pulse integration is employed in scanning radar, the effective signal power of the system increases with the number of pulses returned by the target in a single scan. That number, in turn, increases with the dwell time of the antenna beam on the target. Thus, a low antenna scan rate increases the effective power (up to the point determined by the number of pulses to be integrated).

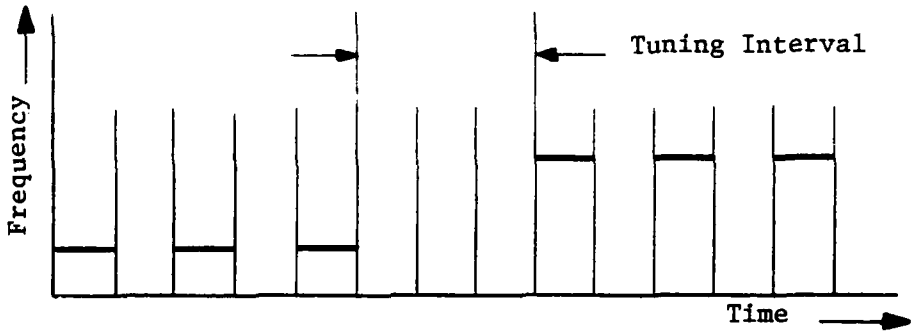
Mainlobe Blanking -- When the direction of a jamming source can be determined, the victim receiver/antenna can be switched off or detuned during that portion of a scan when the antenna mainlobe passes through the direction to the jammer.

Monopulse Detection -- A monopulse radar derives target bearing from the return from a single pulse. Since no antenna scanning is involved, such a system cannot be angle jammed by a jammer utilizing scan-synchronized signals. Furthermore, since only a few pulses are needed for tracking, intermittent operation can be employed to minimize information to the jammer. Such ECM techniques as Cross-Eye, (see Section 2.2.3 of this text), are only marginally effective.

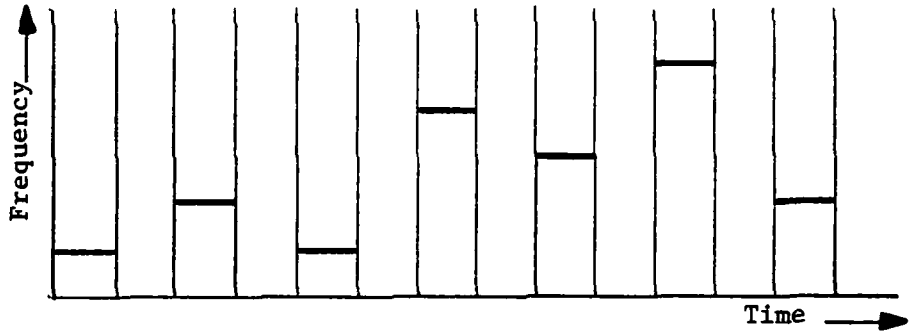
(a) Multiple Frequency System



(b) Fast - Tuning System



(c) Frequency-Agile System



(d) Intra-Pulse FM System

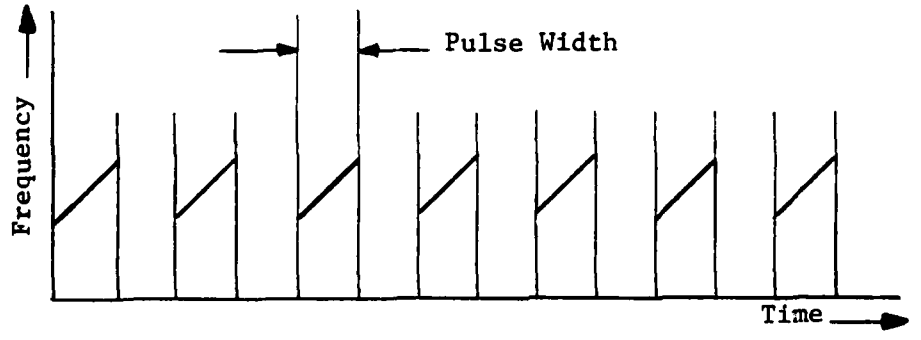


Figure 2.3.3.1 -- Frequency Diversity

Polarization Diversity -- The use of multiple or changing polarization requires that the jammer sense and duplicate the polarization or suffer severe (J/S) reduction at the receiving antenna.

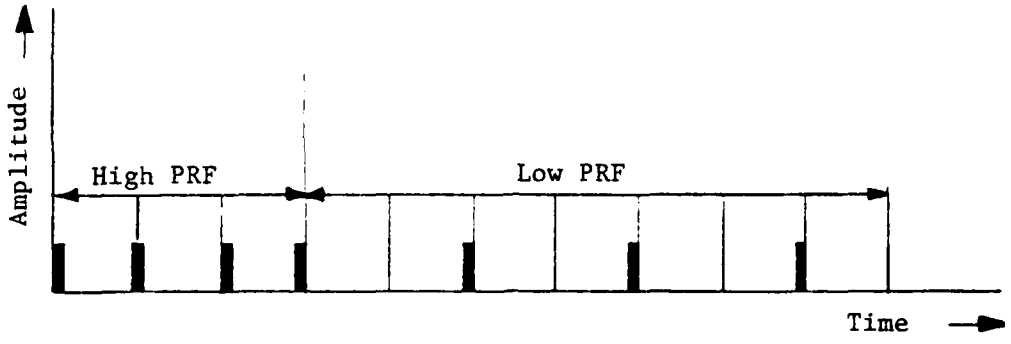
Power Increase -- An increase in transmitted power produces a corresponding increase in (S/J) unless the jammer also increases power.

PRF Diversity -- Diversity in pulse repetition frequency takes one of the three forms illustrated in Figure 2.3.3.2. In a variable PRF system, the PRF of groups of pulses is periodically changed among two or more values according to a fixed program, as shown in part (a) of the figure. In a staggered PRF system, the PRF is alternately switched between two values, on a pulse-to-pulse basis, as shown in part (b) of the figure. In a random PRF system, the PRF is changed, on a pulse-to-pulse basis, between a number of fixed values, according to a pseudo-random program, as shown in part (c) of the figure.

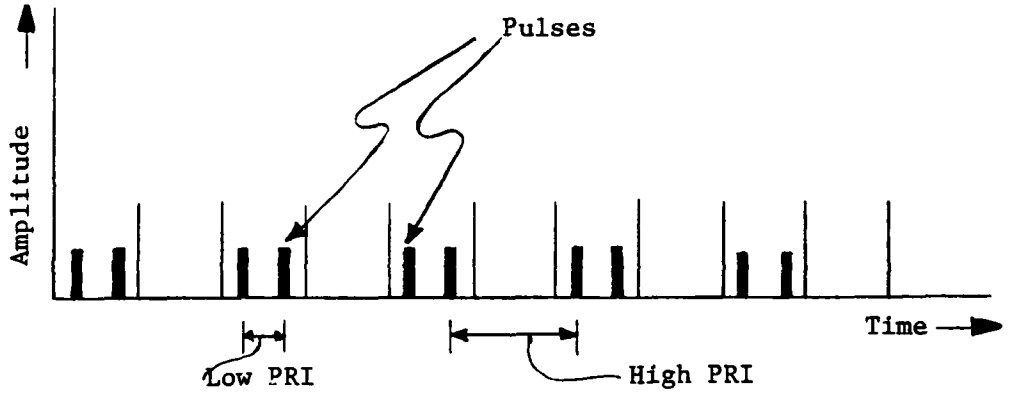
PRF Increase -- For a given radar beam width and scan rate, the PRF determines the number of "hits" on a target in a single scan. In a system employing pulse integration, the number of "hits" determines the effective power in the target return. Thus, in such a scanning radar, a high PRF yields a higher effective power on the target and, generally, a larger signal-to-jamming ratio.

Scan Diversity -- In a scanning radar, changing the scan pattern alters the signal (information) received by the jammer, thus requiring continuous monitoring of the radar signal and modification of the jamming signal. During the "transients" produced by a change of scan pattern, the jamming signal will be ineffective.

(a) Variable PRF System



(b) Staggered PRF System



(c) Random PRF System

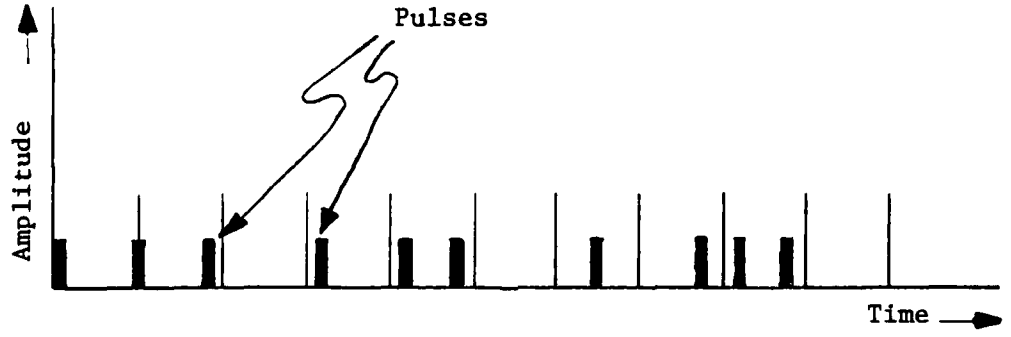


Figure 2.3.3.2 -- PRF Diversity

Scan-on-Receive Only -- By scanning only the receiving antenna, a radar can deny to the jammer knowledge of the scan pattern and interval. Under such circumstances, the jammer cannot employ fixed scan rate modulation jamming as described in Section 2.2.3 of this text. Swept scan rate modulation jamming provides only intermittent disruption of a scanning radar.

Scan Rate Diversity -- Scan rate diversity in a scanning radar requires continuous updating of jamming signal characteristics and produces transient errors in the jamming signal, thus reducing jamming effectiveness.

Sidelobe cancellation -- Cancellation of the signals received in the sidelobes of an antenna can be effected through the use of an omnidirectional "guard" antenna as illustrated in Figure 2.3.3.3. When a signal is received less in the main antenna than in the guard antenna, the signal is rejected. Thus, only signals received in the main lobe of the main antenna will be accepted. Sidelobe cancellation rejects jamming signals injected into the sidelobes of the main antenna.

Sidelobe Reduction -- Reduction of the sidelobes of the system antenna results in a reduced jamming-to-signal power ratio, (J/S), for sidelobe jamming. Reduction of antenna sidelobes is effected by good antenna design and is not necessarily produced by maximizing main lobe gain.

Spread Spectrum Modulation -- Spread spectrum techniques, as discussed in Section 2.5.8 of the communications text, are widely employed in ECCM to encode the information signal and to spread the signal (and jamming) energy over a broad

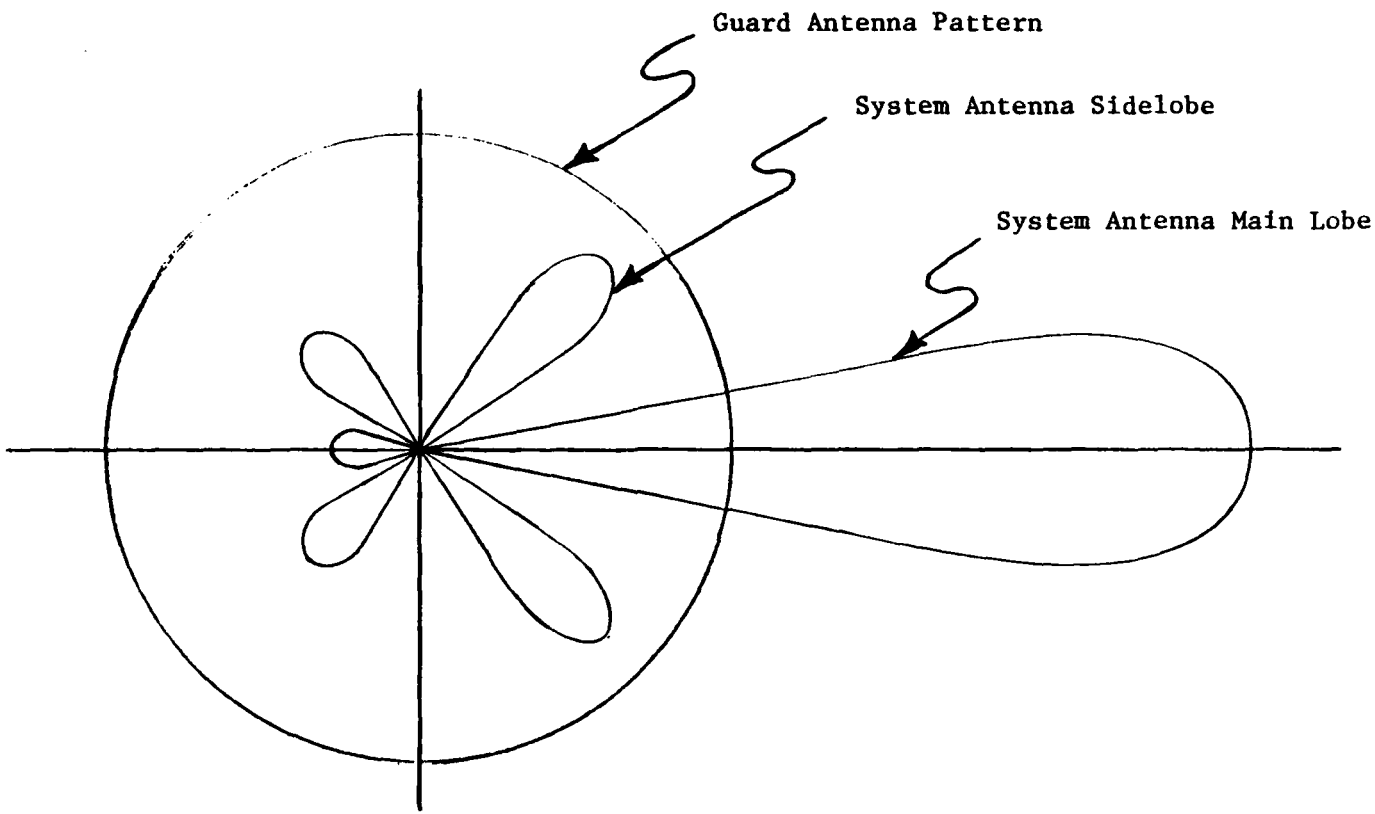


Figure 2.3.3.3 -- Sidelobe Cancellation Antenna Patterns

spectrum. Covert and/or encrypted transmissions can be produced by direct sequence modulation. Pulse energy can be increased by "chirp" modulation (pulse compression). Frequency diversity can be achieved by modulation or frequency hopping. Information signal encoding can be effected by modulation or time hopping, thereby providing the means to employ correlation detection techniques. All of these spread spectrum techniques are discussed in Section 2.5.8 of the communications text.

Receiver/Signal Processor ECCM Techniques

Coherent Signal Processing -- For deception ECM techniques to be effective against a system employing coherent signal processing, the jamming signal must also be coherent. Jamming signal coherence is difficult to achieve, requiring phase control of the carrier in addition to modulation of the signal envelope.

Correlation Detection -- Correlation detection, as discussed in Section 2.5.7 of the communications text, allows discrimination between the information signal and the jamming signal, thereby increasing the post-detection signal-to-jamming power ratio.

Double Threshold Detection -- The use of both upper and lower detection thresholds allows the system to accept only signals the amplitudes of which fall between the two values. The lower limit discriminates against low-level signals such as background noise. The upper limit discriminates against high-level jamming signals.

Dynamic Range Increase -- An increase in the dynamic range, (the range of input amplitudes to which a system will respond), of a receiver prevents large amplitude jamming inputs from driving the receiver into saturation and thereby obscuring the information signal.

Gain Control -- The gain (amplification) of a system can be controlled in such a way that low-amplitude inputs are not lost and high-amplitude inputs do not saturate the system. The gain can be controlled automatically or manually. Unfortunately, low-amplitude information signals may be lost due to the effect of simultaneous large-amplitude jamming signals on the AGC (automatic gain control).

Leading Edge Tracking -- Due to inherent time delays in a pulse repeater utilized in outbound range gate pulloff track breaking, the RGPO (cover) pulse fails to conceal entirely the true target return, as shown in Figure 2.3.3.4. If the jammed system is designed to track the leading edge, (rather than the peak), of the combined pulse, the tracker will follow the target return rather than the RGPO pulse. Leading edge tracking can be defeated by the use of a "cover" pulse which is timed from the previously received radar pulse and extends beyond the target skin return pulse in both directions.

Linearity Improvement -- In a nonlinear receiver, the presence of a large-amplitude jamming signal will reduce the system response to the information signal and also produce transients (false signals). These effects can be eliminated by designing the receiver to have a large linear input range.

Logarithmic Amplification -- Logarithmic amplification, while nonlinear, (see above), prevents receiver recovery transients due to saturation and maintains partial sensitivity to the information signal.

Moving Target Detection -- A moving-target detector is inherently resistant to those forms of ECM, such as chaff, which do not produce false targets with velocities similar to those of the true target.

Noise and Jamming Cancellation -- When an interfering signal can be received alone (without the information signal), it can be subtracted from the combined (information-plus-jamming) signal to yield the information signal alone. In order to receive the interfering signal alone, it must be distinguishable from the information signal on the basis of some characteristic such as amplitude, frequency, modulation, polarization, or direction-of-arrival.

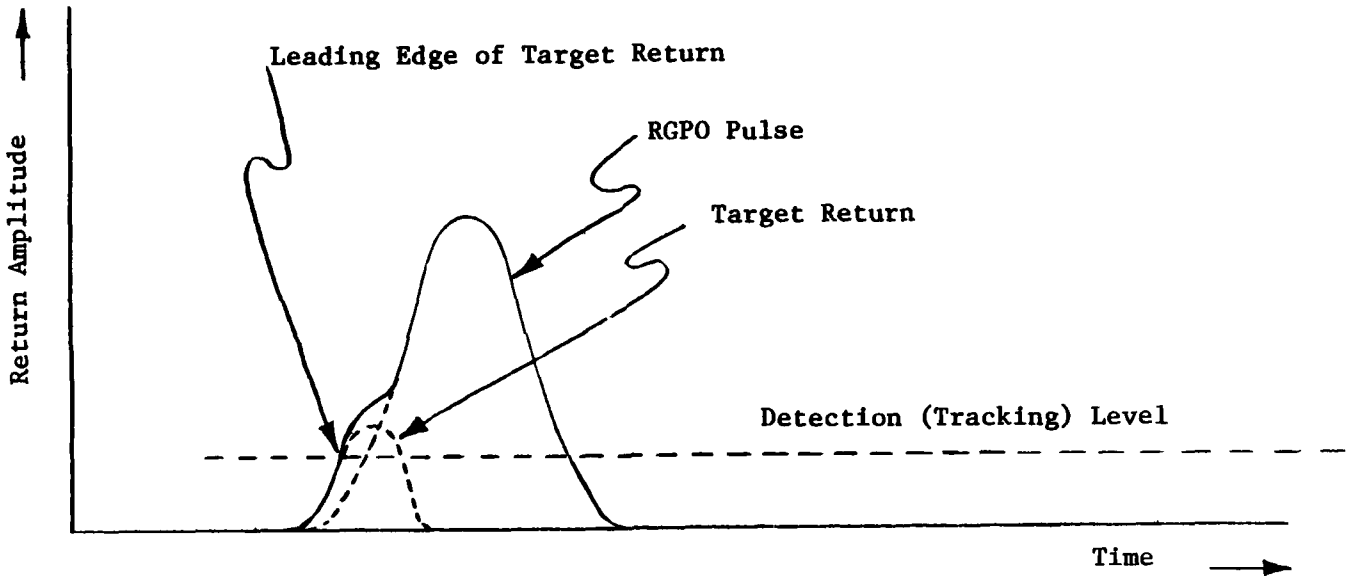


Figure 2.3.3.4 -- Leading Edge Tracking

Pre-detection Frequency Discrimination -- Pre-detection (carrier) frequency filtering can be employed to distinguish between the information and jamming signals when a difference in spectral content exists. Pre-detection frequency filtering is especially effective against ECM techniques, such as skirt and image jamming, that utilize de-tuned carriers.

Predictive Tracking -- Predictive tracking utilizes the continuity in some characteristic (target position, velocity, etc.) to identify the information signal. When a jamming signal does not exhibit that same continuity, it can be distinguished from the information signal on that basis.

Pulse Discrimination -- When the information signal differs from the jamming signal in modulation, (such as pulse size, shape, PRF, etc.), the system can be designed to discriminate between the information and jamming signals on that basis.

Pulse Integration -- Pulse integration, as discussed in Section 2.7 of the radar text, effectively combines the energies contained in the integrated pulses. The target returns possess time coherency and thus add. Non-time-coherent jamming pulses will not add. Thus, the information signal-to-jamming signal power ratio will be increased by the pulse integration.

Range Gating -- The use of a range gate, as discussed in Section 2.14 of the radar text, eliminates all interference received outside the time interval established by the range gate. Thus, the information signal-to-jamming signal ratio encountered by subsequent operations (such as Doppler filtering), is greatly reduced.

Range Resolution Improvement -- An improvement in the range resolution of a radar allows the system to better distinguish between the true target and a deception target on the basis of range (time-of-arrival of the signal).

Shielding -- Electromagnetic shielding reduces the amount of jamming power that can be injected into the system through internal circuitry. (One type of ECM utilizes a jamming signal at the intermediate frequency of the intended victim system.)

Target Return Width Discrimination -- Target return width discrimination distinguishes between the target skin return and the return due to a self-protection pulse repeater on the basis of the apparent angular subtense of the target. The repeater return "target" will appear wider if the repeater threshold level is such that the repeater transmits full power over a wider scan angle than that indicated by the target skin return and the radar threshold sensitivity.

Threshold Detection -- Threshold detection imposes a lower limit on target return amplitude below which signals will not be accepted. The purpose of such a limit is to discriminate against low-level background interference.

Velocity Gating -- The use of a velocity gate, as discussed in Section 2.14 of the radar text, eliminates all interference outside the frequency interval established by the Doppler filter. Thus, the information signal-to-jamming signal power ratio encountered by subsequent operations is greatly reduced.

Wideband Limiting (Dicke Fix) -- Wideband amplification followed by amplitude clipping (limiting) is employed to discriminate against the large-amplitude impulses produced in the victim receiver by FM (swept frequency) noise jamming.

The clipping limits the jamming pulse amplitude to the same order as that of the target return pulses and spreads the spectrum of the jamming pulses so that subsequent narrow band filtering reduces the power of the jamming signal to a level below that of the target returns.

Zero-Crossing Detection -- Zero-crossing detection utilizes the rate at which the composite return signal (target returns plus jamming) goes through zero to detect the presence of a target return. (The presence of a target return will decrease the rate at which zero crossings occur.) Zero crossing detection is more reliable than threshold detection in the presence of strong jamming signals.

Data Processing/Operational ECCM Techniques

Anti-ARM ECM -- The ECM techniques discussed in Section 2.2 of this text, when employed against anti-radiation missiles, can be considered ECCM techniques. (Anti-radiation missiles are both ECM and ECCM devices.)

Aural Detection -- A human operator often can identify jamming signals by the sound of the video modulation.

Decoy Radiators -- Non-functional radiators can be used as decoys to divert ECM activities away from functional systems.

Doppler Velocity/Range Rate Comparison -- The radial velocity of an apparent target can be determined by two independent methods: Doppler frequency shift and rate of change of range. By utilizing both methods and comparing the results, a tracking radar can identify a deception (false) target when velocity discrepancies exist.

Electronic Reconnaissance -- As previously indicated, electronic reconnaissance is an important adjunct to both ECM and ECCM. ECM signals often can be identified on the basis of information obtained by ER.

Human Operator Monitoring and Control -- The capabilities of an experienced operator often determine the outcome of the ECM/ECCM battle. The ability of the human operator to introduce and to recognize novel maneuvers is indispensable in the rapidly evolving field of electronic warfare.

Home-on-Jam Missiles -- When employed against ECM jammers, the home-on-jam missile is an ECCM device.

Manually-Aided Tracking -- A standard ECCM technique employed in tracking radar systems is provision for a manual back-up mode of operation. In the absence of jamming, a human operator cannot track a target as accurately as an automatic tracker. In the presence of jamming, however, he often can outperform an automatic system.

Missile Fuse ECCM -- Anti-missile ECM intended to pre-detonate the missile can be countered by delaying activation of the fuse, (arming of the missile), until just before the detonation point. The delay allows a minimum time after activation in which the jammer can identify the problem and pre-detonate or otherwise jam the missile fuse. When the missile fuse is a radar device, the previously discussed radar ECCM techniques also apply.

Multiple Sensor Tracking -- The use of multiple sensors, (netting), provides ECCM in several ways. The redundant data provide a stronger tracking solution, thereby improving general resistance to jamming. In addition, the jammer may be unable to jam all the trackers in the net, thus allowing the unjammed trackers to provide accurate tracking data. Finally, when jamming destroys target range information but does not conceal target bearing, (as with self-protection noise jamming), two or more trackers can triangulate to obtain a target fix.

Operating Time Minimization -- By minimizing operating time, a system can: (1) deny jamming information to the adversary, and (2) allow minimum time for effective jamming. Both surface-based and airborne radars employ this technique.

Remote Location of Antenna -- Remote location of the transmitting antenna achieves two purposes. First, it allows the separate receiving antenna to avoid a directive jamming signal, (which is generally aimed at the transmitting antenna). Secondly, it draws the fire of anti-radiation missiles, thus sparing the rest of the system.

Sensor Mobility -- Sensor mobility can deny, to the adversary, prior knowledge of the location of the system. For directive jamming or avoidance, such information is required.

Threat Identification -- Positive identification of either the information signal (true target returns) or the jamming signal (false target returns) allows the jammed system to distinguish between the two. Such identification is based upon prior information obtained by electronic reconnaissance.

Tracking Acceleration Limiting -- Limiting the target acceleration (or velocity) accepted by a tracking system, the data processor can reject false targets with physically unrealizeable motion dynamics.

Tracking-on-Jamming Signal -- When self-protection jamming obscures tracking information in the primary tracking mode, an alternate track-on-jam mode can utilize the jammer as a beacon, thereby obtaining target bearing information.

Triangulation -- Two or more non-colocated sensors can be employed to obtain target position utilizing angle-only tracking. (See Multiple-Sensor Tracking).

2.3.4 ECCM Techniques Categorized by Objective

Denial of Information to Adversary

Bistatic Antennas
Frequency Diversity
Monopulse Detection
Operating Time Minimization
Polarization Diversity
PRF Diversity
Remote Location of Antenna
Scan Diversity
Scan-on-Receive Only
Scan Rate Diversity
Sensor Mobility

Avoidance/Reduction of Jamming Signal

Adaptive Antenna
Angular Resolution Improvement
Bistatic Antennas
Coherent Signal Processing
Frequency Diversity
Human Operator
Mainlobe Blanking
Polarization Diversity
Pre-Detection Frequency Discrimination
Range Gating
Range Resolution Improvement
Scan Diversity
Shielding
Sidelobe Cancellation
Sidelobe Reduction
Spread Spectrum Modulation
Velocity Gating

Increase of Effective Signal Power

Antenna Gain Increase
Correlation Detection
Low Scan Rate
Multiple-Sensor Tracking
Power Increase
PRF Increase
Pulse Integration
Spread-Spectrum Modulation

Rejection of False Information

Aural Detection
Coherent Signal Processing
Correlation Detection
Doppler Velocity/Range
Rate Comparison
Frequency Diversity
Human Operator
Leading-Edge Tracking

Manually-Aided Tracking
Moving Target Detection
Multiple-Sensor Tracking
Pre-Detection Frequency Discrimination
Predictive Tracking
PRF Diversity
Pulse Discrimination
Range Gating
Scan Diversity
Scan Rate Diversity
Spread-Spectrum Modulation
Target Identification
Target Return Width Discrimination
Tracking Acceleration Limiting
Velocity Gating

Prevention of Receiver Saturation

Dynamic Range Increase
Gain Control
Linearity Improvement
Logarithmic Amplification
Pre-Detection Frequency Discrimination
Wideband Limiting

Prevention of System Saturation

Double Threshold Detection
Gain Control
Human Operator Monitoring and Control
Moving Target Detection
Multiple-Sensor Tracking
Range Gating
Threshold Detection
Velocity Gating
Zero-Crossing Detection

Maintenance of Signal Tracking

Manually-Aided Tracking
Multiple-Sensor Tracking
Predictive Tracking

2.4 Communication Link Electronic Warfare

2.4.1 EW Techniques -- Nearly all of the principles and techniques previously discussed apply to all types of "communications" systems, including radar, communication links, and radio navigation systems. Only certain specific ECM and ECCM techniques, (such as range-gate pull-off and leading-edge tracking), apply uniquely to radar and other target-tracking sensors. For example, both noise jamming and deception jamming can be employed against all communications systems. In voice communication system jamming, however, deception is very difficult due to the unique characteristics of human voice communication. For the same reason, voice communication jamming sometimes employs the human voice as a jamming signal. In jamming digital data links, random pulses of the same pulse width as those of the information signal are often used. Gaussian noise is sometimes used for both speech and data-link jamming because it resembles natural background noise and may, therefore, go undetected (as jamming). An important ECCM technique for voice and digital data links is time compression, whereby the information signal is compressed in time before transmission in order to achieve minimum operating time. In communication link electronic warfare, the principal purpose of the countermeasure is often to determine the content of the information signal. (In radar EW, the principal purpose is generally to interfere with or obscure the signal.) Because of the stress on information content, encryption assumes an especially important role in communication link ECCM. In this field, the classical techniques of cryptology must be added to the electronic encryption techniques previously discussed.

2.4.2 Jam-to-Signal Ratio for Communication Link Jamming -- The signal power equations for communication link jamming can be derived directly from the communications Equation discussed in Section 2.4.3 of the communications text.

The information signal power (S) and the jamming signal power (J), at the input to the receiver are given by the following equations.

$$S = \frac{P_T G_{TR} G_{RT} \lambda^2}{(4\pi)^2 R_{TR}^2} \quad \text{(Watts)} \qquad 2.4.2.1$$

$$J = \frac{P_J G_{JR} G_{RJ} \lambda^2}{(4\pi)^2 R_{JR}^2} \quad \text{(Watts)} \qquad 2.4.2.2$$

where:

G_{TR} = Gain of transmitting antenna in direction of receiver.

G_{RT} = Gain of receiving antenna in direction of transmitter.

G_{JR} = Gain of jamming antenna in direction of receiver.

G_{RJ} = Gain of receiving antenna in direction of jammer.

P_T = Transmitter Output Power.

P_J = Jammer Output Power.

R_{TR} = Range from transmitter to receiver.

R_{JR} = Range from jammer to receiver.

λ = Radiation wavelength.

At the receiver, the jamming signal-to-information signal power ratio is then:

$$\frac{J}{S} = \frac{P_J G_{JR} G_{RJ} R_{TR}^2}{P_T G_{TR} G_{RT} R_{JR}^2} \quad \text{(N.D.)} \qquad 2.4.2.3$$

Because of the one-way free space attenuation for a communication link, the jammer does not have the advantage it has for radar jamming. For that reason, successful communication link jamming requires that the jammer either be closer to the receiver than is the transmitter or radiate more power in the direction of the receiver than does the transmitter.

2.5 Electro-Optical System Electronic Warfare

Electro-optical systems, (that is, systems operating at optical frequencies), conform to the same basic principles that apply to radio-frequency systems. The hardware differences that exist are a result of the fact that different electromagnetic phenomena predominate in different portions of the electromagnetic spectrum. For the same reason, there exist differences in the testing of radio-frequency and optical-frequency systems. For the most part, however, the discussions on the testing of radio-frequency communication link and radar EW systems apply to their respective counterparts in the optical-frequency domain. The significant differences that exist between EW in radio frequency systems and EW in optical-frequency systems are primarily due to the relatively narrow beamwidth and relatively narrow bandwidth of optical-frequency system radiation. Both characteristics make signal interception and jamming difficult. Theoretically, however, the same EW principles apply.

3.0 Electronic Warfare System Characteristics

3.1 Generic EW System

3.1.1 General Description -- As indicated in the preceding sections of this text, electronic warfare equipment is of five kinds: receivers, transmitters, antennas, signal analyzers, and signal generators. The block diagram of a generalized EW system is shown in Figure 3.1.1.1. In an electronic reconnaissance system, only the receiver and signal analyzer are utilized. In a noise jammer, the signal generator produces a noise-like signal with characteristics determined by the received signal parameters. That noise signal is then amplified and transmitted. In a repeater deception jammer the received pulse is retransmitted with a carrier frequency determined by the RF memory and timing and modulation determined by the signal generator. In a transponder deception jammer, the signal generator produces jamming pulses with characteristics determined by the parameters of the received signal.

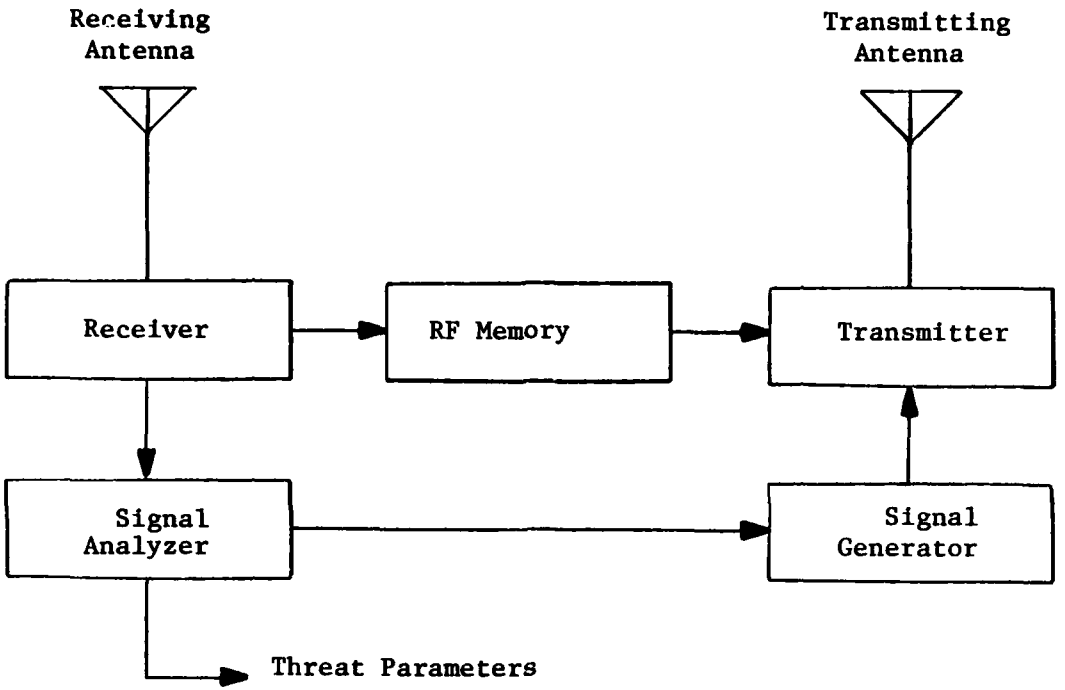


Figure 3.1.1.1 -- Generalized Electronic Warfare System

3.1.2 Electronic Warfare System Requirements -- An electronic warfare system is, of course, a "communications system" as defined in the text on communications systems. For a general discussion of the major functional requirements placed upon communications systems, (including EW systems), the reader is referred to Section 3.1.2 of that text.

3.1.3 Electronic Warfare System Design Features -- For a general discussion of communications system design features, the reader is referred to Section 3.1.3 of the text on communications systems.

3.2 Definitions of Electronic Warfare System Characteristics

3.2.1 Types of EW System Equipment -- As previously indicated, electronic warfare equipment consists of receivers, transmitters, antennas, signal analyzers, and signal generators. For definitions of the general characteristics of communications receivers, transmitters, and antennas, the reader is referred to Section 3.2.2 of the text on communications. The characteristics of EW signal analyzers and generators depend upon the specific nature of the EW system as discussed in the preceding sections of this text.

3.2.2 Specialized Electronic Warfare System Characteristics -- The charateristics relevant to electronic warfare systems are listed below and defined in the following paragraphs.

Electronic Warfare System Characteristics

Antenna Patterns
Blip-to-Scan Ratio
Complex Scenario Performance
Detection Range, Maximum
Detection Range, Minimum
Direction-of-Arrival Determination Accuracy
Dynamic Range
Electromagnetic Compatibility
Electromagnetic Interference
False Alarm Rate
Interference Rejection
Jamming Effectiveness
Jam-to-Signal Ratio
Look-Through Capability
Miss Distance
Parametric Measurement Accuracy
Power Output
Radar Cross Section
Reaction Time
Saturation
Threat Prioritization
Threat Recognition, Basic
Threat Recognition, High Signal Density
Threat Recognition, Multiple Emitter
Threshold Sensitivity, Functional
Transmission Line Loss
Voltage Standing Wave Ratio
Warning Coverage

Antenna Patterns -- The radiation patterns of the receiving and transmitting antennas.

Blip-to-Scan Ratio -- The ratio of the number of aircraft detections achieved per scan by a threat radar.

Complex Scenario Performance -- Threat identification and/or jamming performance in an environment involving many emitters.

Detection Range (Max.) -- The maximum range at which an EW system can detect, identify, and locate a threat emitter. Maximum detection range is determined by system threshold sensitivity.

Detection Range (Min.) -- The minimum range at which an EW system can detect, identify, and locate a threat emitter. Minimum detection range is determined by antenna receiving patterns and receiver saturation.

Direction-of-Arrival Determination Accuracy -- The accuracy with which an EW system determines the direction-of-arrival of the threat signal.

Dynamic Range -- The range of minimum to maximum receiver input signal amplitudes for which the EW system is able to function.

Electromagnetic Compatibility (EMC) -- The ability of an EW system to function properly in conjunction with other equipment without degradation of the performance of either.

Electromagnetic Interference (EMI) -- The degradation of the performance of one system due to the operation of another system.

False-Alarm Rate -- The rate of occurrence of false threat indications.

Interference Rejection -- The ability of an EW system to operate properly in the presence of electromagnetic interference (EMI).

Jamming Effectiveness -- The effectiveness with which an EW system (jammer) interferes with the operation of the victim system. Jamming effectiveness can be measured in terms of reduced probability of detection (for a detection system) miss distance (for a missile) or tracking errors (for a gun director or other tracking system).

Jam-to-Signal Ratio -- The ratio of the jamming signal power to the target return power, at the sensor receiver.

Look-Through Capability -- The ability of an EW receiver/threat analyzer to receive and properly process threat signals during operation of an associated jammer or other signal source.

Miss Distance -- The minimum missile-to-target distance achieved by a (real or simulated) missile.

Parametric Measurement Accuracy -- The accuracy with which an EW system can determine the parameters (frequency, pulse repetition interval, pulse width, pulse modulation, scan rate, etc.) of a threat signal.

Power Output -- The power radiated by an EW jammer.

Radar Cross Section -- The effective radar-signal-reflecting area of the target aircraft. Radar cross section determines the radar target return power and, hence, affects the jam-to-signal ratio.

Reaction Time -- The time interval between the occurrence of a threat emission and threat identification or initiation of jamming, depending on the EW system.

Saturation -- A condition in a signal processing device caused by an input signal too large for proper operation of the device.

Threat Prioritization -- The process of determining and indicating the relative importance (lethality) of a number of simultaneous threats, according to previously established criteria.

Threat Recognition, Basic -- The ability of an EW system to identify and locate threat emissions with no other signals present.

Threat Recognition, High Signal Density -- The ability of an EW system to identify and locate threat emissions in the present of numerous simultaneous signals.

Threat Recognition, Multiple Emitter -- The ability of an EW system to identify and locate more than one threat emission simultaneously.

Threshold Sensitivity, Functional -- The minimum input signal amplitude sufficient to allow an EW system to identify and locate the threat emitter.

Transmission Line Loss -- The attenuation of a signal due to propagation along an energy-dissipating transmission line.

Voltage Standing Wave Ratio (VSWR) -- The ratio of maximum to minimum signal voltages along a transmission line with both forward and reflected waves. VSWR is a measure of reflected power or impedance mismatch in the line.

Warning Coverage -- The range of relative bearings for which an EW system proper'y detects, identifies, and locates a threat emitter.

3.3 Specific EW Systems

The characteristics of existing specific electronic warfare systems are classified and are, therefore, not included in this text. For that information, the reader is referred to the separate, classified volume on Airborne Systems Descriptions.

4.0 Electronic Warfare System Performance Test and Evaluation

4.1 The Philosophy of Testing

As previously indicated, an electronic warfare system is a type of communications system. For a general discussion of the philosophy of communications systems testing, the reader is referred to Section 4.1 of the text on Communications Systems.

4.2 The Nature of EW System Testing

The testing of electronic warfare systems consists, in part, of the testing of system components, (receivers, transmitters, antennas, signal analyzers, and signal generators), as components. For a discussion of the testing of transmitters, receivers, and antennas, as such, the reader is referred to Sections 4.2, 4.3, and 4.4 of the text on Communications Systems, respectively. In addition, when the EW system to be tested is a radar deception jammer, the reader is referred to Section 4.2 of the text on Radar Systems for discussions of measurement techniques for determining radar signal parameters such as pulse width and pulse repetition frequency.

Electronic counter-countermeasures (ECCM) hardware is, of course, an integral part of the system to be protected (communications set, radar set, etc.). For that reason, the testing of ECCM hardware is performed utilizing the tests described in the texts devoted to the specific type of system.

The functional testing of specialized EW signal analyzers and generators and other EW-peculiar testing is best performed in integrated EW system tests. Such tests are discussed in the following paragraphs.

4.3 EWISTL - The Electronic Warfare Integrated Systems Test Laboratory

At the Naval Air Test Center, integrated EW systems ground testing is performed in the Electronic Warfare Integrated Systems Test Laboratory (EWISTL). The EWISTL consists primarily of a complex signal generator, an EW system signal monitor, and a computer-controlled scenario simulator. The signal generator produces simulated threat signals with which to excite the EW system under test. The signal monitor records and reduces test data, including the response signals from the EW system under test. The scenario simulator varies the characteristics of the simulated threat signals to simulate the composite signal environment experienced by an EW system mounted on a platform moving through a field of up to 255 moving or stationary threat emitters.

The simulated threat signals can be injected into the EW system under test either by RF couplers inserted just beyond the antenna (non-radiative coupling) or by injecting video signals just beyond the first detector. In either case, the radiative characteristics of the antennas are not measured in the EWISTL tests. (The antenna radiation patterns are determined in other testing). It is planned eventually to add radiative coupling in an anechoic chamber to the EWISTL capabilities.

The output (response) signals of the EW system under test are generally transmitted to the EWISTL data processor by monitoring the existing output data lines or data bus. Special instrumentation also can be provided to monitor the RF responses of the EW system.

The signal generator is capable of simulating the emissions of up to 1000 individual emitters, (up to about 300 at any one time), with a total composite pulse rate up to about 3,000,000 pulses per second. Special modulations can be applied to the signals, such as frequency agility, PRF agility, pulse modulation, and pulse code modulation. The parameter ranges of the simulated threat signals are listed below.

Frequency: 0.5 to 18 GHz
Pulse Rate: 250 to 100,000 PPS
Pulse Width: 0.1 to 100 μ sec
Scan Type: Circular, Sector, Conical, Raster, Fixed
Scan Rate: 2 to 2700 RPM

The EWISTL provides the capability of testing integrated EW systems in a realistic, repeatable scenario with simulated threat signals designed to test the ability of the EW system to identify and locate specific, multiple threats in a high-emitter-density, high-pulse-rate environment. The test data are automatically reduced to yield the performance characteristics of the EW system under test, including those listed below.

Threat Recognition Capability
Threat Density Limitations
Signal Parameter Limitations
Threat Prioritization Performance
Threat Reaction Time
False Alarm Rate
EMI/EMC Effects

A functional block diagram of the EWISTL is shown in Figure 4.3.0.1.

4.4 Electronic Warfare System Performance Test Methods

4.4.1 Laboratory (EWISTL) Tests -- The following tests are conducted in the EWISTL facility, with pre-planned test scenarios, as described in Section 4.3 of this text.

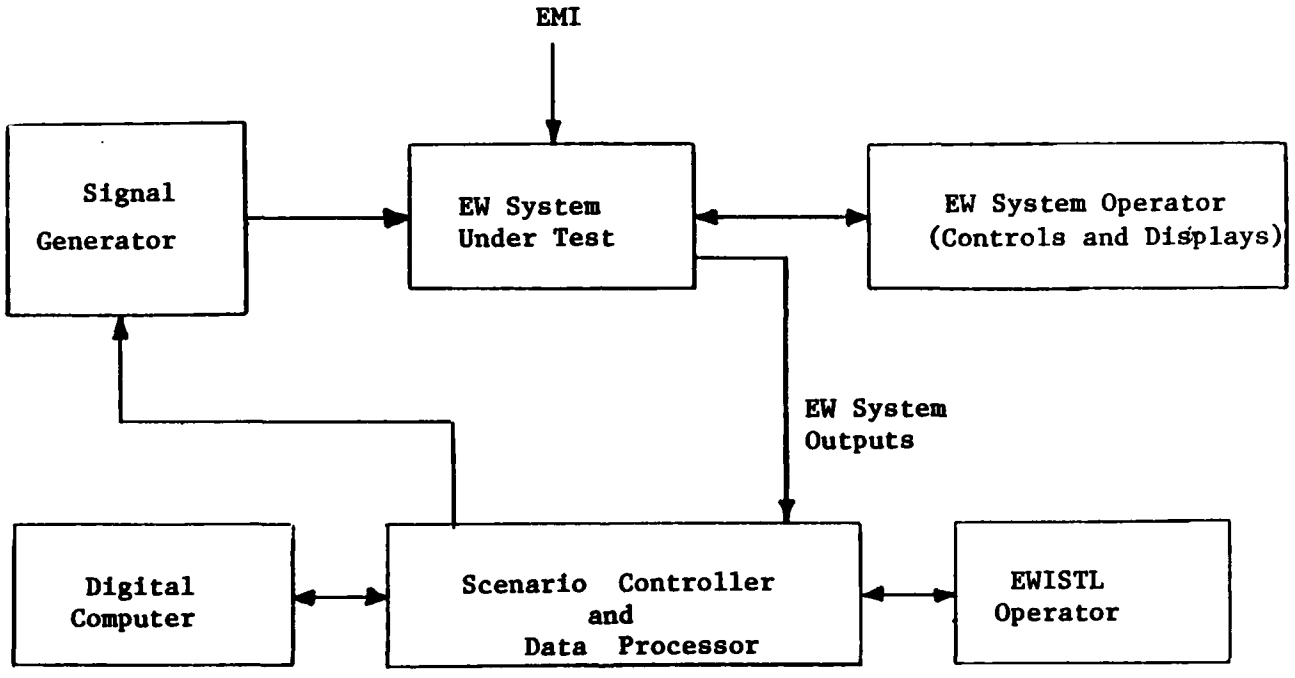


Figure 4.3.0.1 -- The Electronic Warfare Integrated Systems Test Laboratory (EWISTL)

Complex Scenario Performance
Direction-of-Arrival Determination Accuracy
Dynamic Range
Electromagnetic Compatibility
Electromagnetic Interference
False Alarm Rate
Look-Through Capability
Parametric Measurement Accuracy
Reaction Time
Saturation
Threat Prioritization
Threat Recognition, Basic
Threat Recognition, High Threat Density
Threat Recognition, Multiple Threat
Threshold Sensitivity
Warning Coverage

4.4.2 Simulated Threat Flight Test Range Tests -- The following flight tests are conducted on a range incorporating functional simulations of known and projected threat systems. Both the effect of the threat signals on the EW system under test and the effect of EW system jamming signals on the threat system are evaluated.

Blip-to-Scan Ratio (Probability of Detection)
Detection Range, Maximum
Detection Range, Minimum
Electromagnetic Compatibility
Electromagnetic Interference
Jamming Effectiveness
Jam-to-Signal Ratio
Look-Through Capability
Miss Distance
Threat Prioritization
Threat Recognition, Basic
Threat Recognition, Multiple
Warning Coverage

4.4.3 Other Tests -- The following tests, part of EW testing but not peculiar to EW systems are described in Section 4.0 of the text on communications systems.

Antenna Patterns
Power Output
Pulse Modulation
Radar Cross Section
Transmission Line Loss
Voltage Standing Wave Ratio